การประเมินระดับความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร จากการอ้างอิงมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ CIA และ ISO 27001:2013 กรณีศึกษา สถาบันการอาชีวศึกษาภาคเหนือ 2

รสริน ศิริรักษ์

การศึกษาค้นคว้าด้วยตนเองเสนอเป็นส่วนหนึ่งของการศึกษา

หลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาการจัดการเทคโนโลยีสารสนเทศสมัยใหม่

มีนาคม 2567

การประเมินระดับความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร จากการอ้างอิงมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ CIA และ ISO 27001:2013 กรณีศึกษา สถาบันการอาชีวศึกษาภาคเหนือ 2

รสริน ศิริรักษ์

การศึกษาค้นคว้าด้วยตนเองเสนอเป็นส่วนหนึ่งของการศึกษา
หลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาการจัดการเทคโนโลยีสารสนเทศสมัยใหม่
มีนาคม 2567

ASSESSMENT OF THE LEVEL OF RISK IN THE USE OF INFORMATION TECHNOLOGY IN THE ORGANIZATION FROM REFERENCE TO CIA BASIC SECURITY AND ISO 27001:2013 CASE STUDY : INSTITUTE OF VOCATIONAL EDUCATION NORTHERN REGION 2

ROSRIN SIRIRUK

An Independent Study Submitted in Partial Fulfillment

of the Requirements for the Master of Science Program Degree

in Modern Information Technology Management

March 2024

การศึกษาค้นคว้าด้วยตนเอง

เรื่อง

การประเมินระดับความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร จากการอ้างอิงมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ CIA และ ISO 27001:2013 กรณีศึกษา สถาบันการอาชีวศึกษาภาคเหนือ 2

ของ รสริน ศิริรักษ์

ได้รับพิจารณาอนุมัติให้เป็นส่วนหนึ่งของการศึกษา
หลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศสมัยใหม่
ของมหาวิทยาลัยพะเยา

..... อาจารย์ที่ปรึกษาการศึกษาค้นคว้าด้วยตนเอง
(ดร. เกวรินทร์ จันทร์ดำ)

..... อาจารย์บัณฑิตศึกษามหาวิทยาลัยพะเยา
(ผู้ช่วยศาสตราจารย์ ดร. บวรศักดิ์ ศรีสังสิทธิสันติ)

..... อาจารย์บัณฑิตศึกษามหาวิทยาลัยพะเยา
(ผู้ช่วยศาสตราจารย์ ดร. สาคร เมฆรักษาวนิช)

..... คณบดีคณะเทคโนโลยีสารสนเทศและการสื่อสาร
(ผู้ช่วยศาสตราจารย์ ดร. พรเทพ โรจนวสุ)

เรื่อง: การประเมินระดับความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร จากการอ้างอิงมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ CIA และ ISO 27001:2013 กรณีศึกษา สถาบันการอาชีวศึกษาภาคเหนือ 2

ผู้ศึกษาค้นคว้า: รสริน ศิริรักษ์, การศึกษาค้นคว้าด้วยตนเอง: วท.ม. (การจัดการเทคโนโลยีสารสนเทศสมัยใหม่), มหาวิทยาลัยพะเยา, 2566

อาจารย์ที่ปรึกษา: ดร. เกวรินทร์ จันทร์ดำ

คำสำคัญ:

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาและพัฒนาเครื่องมือวัดระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กรโดยอ้างอิงมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขั้นพื้นฐาน CIA และ มาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ได้รับการยอมรับระดับสากล ISO 27001 : 2013 และ 2) เพื่อศึกษาระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กรของสถาบันการอาชีวศึกษาภาคเหนือ 2 และสถานศึกษาในสังกัด จำนวน 9 แห่ง

ผลการวิจัยพบว่า 1) กลุ่มตัวอย่าง สถาบันการอาชีวศึกษาภาคเหนือ 2 มีระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กร ในระดับความเสี่ยง สูงมาก 2) กลุ่มผู้ใช้งาน สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 จำนวน 9 แห่ง มีผลการประเมินระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กร ได้แก่ วิทยาลัยเทคนิคเชียงราย มีระดับความเสี่ยง สูง วิทยาลัยอาชีวศึกษาเชียงราย มีระดับความเสี่ยงปานกลาง วิทยาลัยเทคนิคกาญจนาภิเษกเชียงราย มีระดับความเสี่ยง สูง วิทยาลัยเทคนิคพะเยา มีระดับความเสี่ยงสูงมาก วิทยาลัยเกษตรและเทคโนโลยีพะเยา มีระดับความเสี่ยง สูง วิทยาลัยเทคนิคแพร่ มีระดับความเสี่ยงปานกลาง วิทยาลัยอาชีวศึกษาแพร่ มีระดับความเสี่ยง ปานกลาง วิทยาลัยเกษตรและเทคโนโลยีแพร่ มีระดับความเสี่ยงสูงมาก และวิทยาลัยเทคนิคน่าน มีระดับความเสี่ยง สูง

Title: ASSESSMENT OF THE LEVEL OF RISK IN THE USE OF INFORMATION TECHNOLOGY IN THE ORGANIZATION FROM REFERENCE TO CIA BASIC SECURITY AND ISO 27001:2013 CASE STUDY : INSTITUTE OF VOCATIONAL EDUCATION NORTHERN REGION 2

Author: Rosrin Siriruk, Independent Study: M.Sc. (Modern Information Technology Management), University of Phayao, 2023

Advisor: Keawarin Jandum

Keywords:

ABSTRACT

The objectives of this research are to study and develop tools to measure risk levels from Use information technology in the organization by CIA basic security and ISO 27001:2013 which is accepted by international standards and study the level of risk from the use of information technology in the organization of the Institute of Vocational education Northern Region 2 and affiliated educational institutions, totaling 9 locations. it is the found that 1) Sample Vocational education Northern Region 2 There is a very high level of risk, and 2) User group is 9 affiliated Vocational education Northern Region 2 ChiangRai Technical College There is a high level of risk, ChiangRai Vocational College There is a medium, level of risk, Kanchanapisek Chianrai Technical College There is a high level of risk, Phayao Technical College There is a very high level of risk, Phayao College of Agriculture and technology There is a high level of risk, Phrae Technical College There is a medium level of risk, Phrae Vocational College There is a medium level of risk, Phrae College of Agriculture and technology There is a very high level of risk, and Nan Technical College There is a high level of risk,

กิตติกรรมประกาศ

ตลอดการศึกษาค้นคว้าด้วยตนเองที่ผ่านมาจนสำเร็จลุล่วงผ่านไปได้ด้วยดี เกิดเป็นชิ้นงานวิจัยที่สมบูรณ์ ผู้ศึกษาขอขอบคุณคณาจารย์ทุกท่านที่ถ่ายทอดความรู้ให้คำแนะนำและให้ความช่วยเหลือตลอดการศึกษา ขอขอบคุณ ดร.เกวรินท์ จันทร์ดำ อาจารย์ที่ปรึกษา–ผู้สอน รองศาสตราจารย์ ดร.สาคร เมฆรักษาวนิช ผู้ช่วยศาสตราจารย์ ดร.บวรศักดิ์ ศรีสังสิทธิสันติ คณะกรรมการที่ชี้แนะคำแนะนำ ทำให้งานศึกษาค้นคว้านี้มีสมบูรณ์มากยิ่งขึ้นขอบคุณ อาจารย์พิเศษ ดร.ธนทรรศน์ แซ่ลิ้ม ผู้สอนรายวิชาความมั่นคงปลอดภัย ฯ ดร.ไกรลาศ ดอนชัย ที่ปรึกษาด้านการประเมินความเสี่ยง ที่คอยให้คำปรึกษา นายบุญธรรม เกี้ยวฝั้น ผู้อำนวยการสถาบันการอาชีวศึกษาภาคเหนือ 2 ที่ให้ความอนุเคราะห์ในการสำรวจ เก็บข้อมูลและคำแนะนำตลอดการศึกษา นายนิวัฒนา คำหล่อ ข้าราชการชำนาญการพิเศษที่คอยให้คำแนะนำในการจัดทำผลการศึกษา ตลอดจนผู้มีส่วนเกี่ยวข้องกับผู้ศึกษาค้นคว้า ทุกท่าน ที่มีส่วนช่วยให้งานศึกษาค้นคว้านี้สำเร็จลุล่วงผ่านไปได้ด้วยดี

หวังเป็นอย่างยิ่งว่า การศึกษาค้นคว้านี้จะเป็นประโยชน์ไม่มากก็น้อยแก่ผู้ศึกษา หน่วยงาน องค์กร ในการนำไปปรับประยุกต์ พัฒนา สร้างสรรค์ให้เกิดชิ้นงานที่มีคุณภาพอื่น ๆ ต่อไป

รสริน ศิริรักษ์

สารบัญ

หน้า

สาบัญตาราง

หน้า

สารบัญภาพ

หน้า

บทที่ 1

บทนำ

ความเป็นมาและความสำคัญของปัญหา

ด้วยสภาวะปัจจุบันภัยทางด้านไซเบอร์หรือโลกออนไลน์ได้สร้างความสูญเสียให้กับประชาชนเป็นอย่างมาก ยิ่งโลกมีการพัฒนาในด้านเทคโนโลยีมากเท่าไหร่ ก็ทำให้ประชาชนต้องมีการปรับตัวให้เข้ากับยุคที่เปลี่ยนแปลงไปอย่างรวดเร็วและปฏิเสธไม่ได้สำหรับการใช้งานเครื่องมืออิเล็กทรอนิกส์ที่ทำหน้าที่ในการเชื่อมโยงเครือข่ายระบบออนไลน์ที่คอยอำนวยความสะดวก สร้างความรวดเร็ว ลดเวลาและลดขั้นตอนในชีวิตประจำวันเป็นอย่างมาก หากเทียบกับยุคก่อน แต่ในขณะเดียวกันเราก็มักจะทราบข่าวการถูกโจรกรรมทางไซเบอร์ หรือการขโมยข้อมูลส่วนตัวของผู้ใช้งานจนทำให้เกิดความสูญเสียและได้รับความเสียหายเป็นอย่างมาก ไม่เว้นเฉพาะข้อมูลส่วนบุคคลเท่านั้น หากกล่าวถึงในระดับองค์กร ข้อมูลต่าง ๆ ขององค์กรถือเป็นหัวใจสำคัญหลัก คือ ทรัพย์สินที่มีมูลค่าขององค์กรก็ว่าได้ สิ่งหนึ่งที่เราทุกคนทราบกันดีว่าการดำรงชีวิตในยุคปัจจุบันส่วนมากจะเลือกการทำงานหรือใช้ชีวิตผ่านระบบออนไลน์ที่มีความรวดเร็ว ง่าย และอำนวยความสะดวกในด้านต่าง ๆ ให้เรา จึงทำให้คนส่วนใหญ่ยอมให้โลกออนไลน์เข้ามาเป็นส่วนหนึ่งในการดำเนินชีวิต โดยการใช้ประโยชน์จากเทคโนโลยีนั้นจะมีทั้งกลุ่มผู้ใช้งานที่มีความระมัดระวังและศึกษาความรู้จากการใช้งานเทคโนโลยีสารสนเทศให้มีความปลอดภัย หมั่นอัพเดตข้อมูลความรู้อย่างสม่ำเสมอไม่ประมาท จึงทำให้สามารถปกป้องข้อมูลส่วนตัวและข้อมูลขององค์กรได้ในระดับหนึ่ง ส่วนอีกกลุ่มผู้ใช้งานจะเป็นกลุ่มที่ขาดความรู้ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศให้เกิดความปลอดภัยก็อาจนำมาซึ่งความสูญเสียและสร้างความเสียหายให้กับตนเองและองค์กรได้ ทั้งนี้ ขึ้นอยู่กับพฤติกรรมการใช้งานของแต่ละบุคคลว่า จะนำไปสู่ความเสี่ยงมากน้อยเพียงใด และจะดีกว่าถ้าผู้ใช้งานสามารถรับรู้และรับทราบระดับความเสี่ยงของตนเองจากการใช้งานเทคโนโลยีสารสนเทศเพื่อจะได้นำไปปรับปรุงและพัฒนาตนเองในการใช้งานเทคโนโลยีสารสนเทศให้มีความปลอดภัยมากขึ้น

หากกล่าวถึงระดับความเสี่ยงหรือระดับความเสียหายที่มีผลกระทบต่อองค์กรนั้น องค์กรขนาดใหญ่จะมีมูลค่าความเสียหายจำนวนมากหากเกิดเหตุการณ์ความไม่มั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขึ้น จึงนำไปสู่การจัดการและสร้างระบบป้องกันความเสี่ยงหรือความเสียหายทางด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพมากกว่า องค์กรขนาดเล็กในขณะที่ค่าใช้จ่ายในการสร้างระบบป้องกันความเสี่ยงฯ รวมถึงค่าใช้จ่ายของผู้ดูแลระบบ

การรักษาความปลอดภัยข้อมูลองค์กรย่อมมีอัตราค่อนข้างสูงตามไปด้วย ฉะนั้นเมื่อมีการลงทุนจำนวนมากและมีความคุ้มค่าต่อการรักษาผลประโยชน์ขององค์กรในภาพรวม จึงย่อมคุ้มค่ากว่าการสูญเสียหากเกิดเหตุการณ์ไม่คาดคิดแน่นอน แล้วองค์กรขนาดเล็กจะมีวิธีการอย่างไรในการปกป้องรักษาข้อมูลของตนเอง อาจจะไม่คุ้มค่าหากต้องลงทุนในระบบเท่ากับองค์กรขนาดใหญ่ดังที่กล่าวมาข้างต้น หากแต่องค์กรขนาดเล็กจะมีการจัดการเฝ้าระวังและมีนโยบายมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่ดี รวมถึงบุคลากรในองค์กรสนับสนุนและร่วมมือด้วยก็จะสามารถทำให้องค์กรขนาดเล็กมีความมั่นคงปลอดภัยได้ในระดับหนึ่งเช่นกัน และน่าจะดีกว่านี้ถ้าองค์กรขนาดเล็กสามารถรับรู้ได้ถึงระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศของบุคลากรในองค์กรซึ่งเป็นกลุ่มขับเคลื่อนองค์กรนั้น ๆ แต่ในข้อเท็จจริงแล้วเป็นที่น่าเสียดายว่า องค์กรขนาดเล็กและหน่วยงานราชการบางส่วนยังขาดการตระหนักรู้ในการปกป้องรักษาข้อมูลขององค์กรและยังขาดความรู้ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศในองค์กร ดังกรณีที่ผู้วิจัยได้ทำการสำรวจและสอบถามข้อมูลจากองค์กรที่ผู้วิจัยทำงานอยู่ พบว่า องค์กรไม่มีมาตรการและนโยบายที่เกี่ยวข้องหรือส่งเสริมให้มีการรักษาความมั่นคงปลอดภัยข้อมูลขององค์กรเลย

จากปัญหาดังกล่าว ผู้วิจัยจึงได้ทำการศึกษาบริบทขององค์กรเพื่อหาแนวทางหรือมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูล ทั้งนี้ การที่องค์กรจะมีระบบป้องกันและรักษาข้อมูลให้มีความมั่นคงปลอดภัยนั้น ก็ต้องมาจากพฤติกรรมการใช้งานเทคโนโลยีสารสนเทศของบุคลากรในองค์กร ซึ่งผู้วิจัยได้พบกับเสาหลักของมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เป็นพื้นฐาน ได้แก่ มาตรฐาน CIA และมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ได้รับการยอมรับในระดับสากล ได้แก่ มาตรฐาน ISO 27001:2013 จึงได้นำมาอ้างอิงเป็นข้อมูลในการสร้างเครื่องมือประเมินความเสี่ยงขึ้น โดยมีการปรับเนื้อหาให้เข้ากับบริบทของสถาบันการอาชีวศึกษาภาคเหนือ 2 จากนั้นได้ให้ผู้เชี่ยวชาญตรวจหาค่า IOC ของเครื่องมือแบบทดสอบ พร้อมศึกษาข้อมูลเกี่ยวกับการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เกณฑ์ระดับการวัด เพื่อให้เครื่องมือในการประเมินมีผลการประเมินที่ตรงกับความเป็นจริงมากที่สุด จากนั้นได้ทำการศึกษาระบบหรือโปรแกรมที่จะนำเครื่องมือการประเมินไปใส่เพื่อให้ผู้ใช้งานสามารถใช้งานผ่านอุปกรณ์หรือเครื่องมือผ่านระบบออนไลน์ได้ อีกทั้งยังเป็นการเก็บรวบรวมข้อมูลการประเมินไว้ในระบบ สามารถใช้เป็นข้อมูลนำเสนอต่อผู้บริหารเพื่อหาแนวทางป้องกันหรือแนวทางดำเนินการแก้ไขปัญหาได้ แต่ปัจจุบันไม่พบระบบหรือโปรแกรมใดที่สามารถตอบสนองความต้องการของผู้วิจัยได้ จึงได้ทดลองออกแบบระบบการใช้งานขึ้นโดยให้ผู้ที่มีทักษะ

ด้านการจัดทำโปรแกรมดำเนินการสร้างระบบที่มีชื่อว่า ITRSM ขึ้น เพื่อให้สามารถใช้งานได้จริง

สถาบันการอาชีวศึกษาภาคเหนือ 2 เป็นหน่วยงานในสังกัด สำนักงานคณะกรรมการการอาชีวศึกษา กระทรวงศึกษาธิการ มีหน้าที่ในการดำเนินงานสนับสนุนการจัดการศึกษาในระดับ ประกาศนียบัตรวิชาชีพ ประกาศนียบัตรวิชาชีพชั้นสูง และระดับปริญญาตรี ปัจจุบันมีสถานศึกษาในสังกัด จำนวน 9 แห่ง 4 จังหวัด คือ เชียงราย พะเยา แพร่ น่าน โดยมีสถานศึกษา ได้แก่ วิทยาลัยเทคนิคเชียงราย วิทยาลัยอาชีวศึกษาเชียงราย วิทยาลัยเทคนิคกาญจนาภิเษกเชียงราย วิทยาลัยเทคนิคพะเยา วิทยาลัยเกษตรและเทคโนโลยีพะเยา วิทยาลัยเทคนิคแพร่ วิทยาลัยอาชีวศึกษาแพร่ วิทยาลัยเกษตรและเทคโนโลยีแพร่ และวิทยาลัยเทคนิคน่าน ในการดำเนินงานสถาบันการอาชีวศึกษาภาคเหนือ 2 มีหน่วยงานที่ต้องทำการเชื่อมต่อและประสานงานด้านสารสนเทศ คือ สำนักงานคณะกรรมการการอาชีวศึกษา สังกัดกระทรวงศึกษาธิการ ซึ่งเป็นหน่วยงานต้นสังกัด และประสานงานกับสถานศึกษาในสังกัดทั้ง 9 แห่ง โดยการรับส่งสารสนเทศระหว่างองค์กร ผ่านระบบอินเตอร์เน็ตเป็นส่วนใหญ่ อีกทั้งมีการดำเนินการจัดเก็บข้อมูลสารสนเทศแต่ละส่วนงานอีกจำนวนมากในแต่ละรอบปีการศึกษา ส่งผลให้การดำเนินงานที่ผ่านมาเจ้าหน้าที่ขององค์กรล้วนต่างทำหน้าที่ของตนตามธรรมเนียมที่เคยปฏิบัติมา ซึ่งผู้วิจัยได้ทำการสอบถามและสังเกตการณ์ดำเนินงานของแต่ละส่วนงาน พบว่า ยังขาดการบริหารจัดการข้อมูลสารสนเทศและขาดการตระหนักรู้ความเข้าใจในการรักษาข้อมูลสารสนเทศขององค์กรอย่างแท้จริง จึงได้ทำการศึกษาบริบทการทำงานขององค์กรตั้งแต่การบริหารงานของผู้บริหาร เจ้าหน้าที่ผู้เกี่ยวข้องในองค์กรที่มีหน้าที่ในการใช้งานเทคโนโลยีสารสนเทศเพียงอย่างเดียวและเจ้าหน้าที่ที่มีหน้าที่ในการดูแลระบบการใช้งานเทคโนโลยีสารสนเทศในองค์กร ทำให้ทราบว่าองค์กรยังไม่ทราบถึงระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ผู้วิจัย ผู้บริหาร ตลอดจนบุคลากรภายในองค์กรทราบถึงระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศ จึงกำหนดกลุ่มตัวอย่างในการวิจัยออกเป็น กลุ่มผู้ใช้งานทั่วไป ที่ทำหน้าที่ในการใช้งานเทคโนโลยีสารสนเทศเพียงอย่างเดียว เหมาะที่จะนำมาตรฐานความปลอดภัย CIA มาเป็นแนวทางกำหนดสร้างแบบทดสอบ เพราะผู้ใช้งานทั่วไปกลุ่มนี้ไม่มีความรู้ทางด้านเทคโนโลยีสารสนเทศโดยตรง และมีเกี่ยวข้องกับการใช้งานเพียงส่วนที่ตนเองรับผิดชอบเท่านั้น ส่วนอีกหนึ่งกลุ่มจะเป็นเจ้าหน้าที่ดูแลระบบสารสนเทศทั้งหมดภายในองค์กร รวมถึงการเชื่อมต่อกับหน่วยงานองค์กรภายนอกด้วย อีกทั้งเป็นผู้มีความรู้และทักษะเชี่ยวชาญเฉพาะด้าน จึงได้นำเกณฑ์มาตรฐาน ISO 27001:2013 มาเป็นเกณฑ์กำหนดสร้างแบบทดสอบที่สอดคล้องและเหมาะสม ตามหัวข้อหลัก 14 หัวข้อ ดังนั้น อาจกล่าวโดยสรุปได้ว่า แบบทดสอบ

จึงมีอยู่ 2 ชุด คือ สำหรับผู้ใช้งานทั่วไปและเจ้าหน้าที่ดูแลระบบสารสนเทศองค์กร โดยคาดหวังเป็นอย่างยิ่งว่า แบบทดสอบและระบบโปรแกรม ITRSM ที่ผู้วิจัยสร้างขึ้นจะมีส่วนในการผลักดันให้เกิดการพัฒนาเครื่องมือประเมินระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศให้แก่องค์กรอื่น ๆ ในอนาคตต่อไป

วัตถุประสงค์

1. เพื่อศึกษาและพัฒนาเครื่องมือวัดระดับความเสี่ยงการจากใช้งานเทคโนโลยีสารสนเทศในองค์กรจากการอ้างอิงมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขั้นพื้นฐาน CIA และ มาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ได้รับการยอมรับในระดับสากล ISO 27001:2013

2. เพื่อศึกษาระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กรของสถาบันการอาชีวศึกษาภาคเหนือ 2 และสถานศึกษาในสังกัด จำนวน 9 แห่ง

ขอบเขตการวิจัย

1. ขอบเขตประชากร

1.1 กลุ่มตัวอย่าง

บุคลากรในองค์กรสถาบันการอาชีวศึกษาภาคเหนือ 2 ประกอบด้วย

1.1.1 กลุ่มผู้ใช้งานทั่วไป จำนวน 10 คน

1.1.2 กลุ่มผู้ดูแลระบบ จำนวน 1 คน

1.2 กลุ่มผู้ใช้งาน

บุคลากรสถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 จำนวน 9 แห่ง แบ่งเป็น

1.2.1 กลุ่มผู้ใช้งานทั่วไป สถานศึกษาละ 10 คน รวม 90 คน

1.2.2 กลุ่มผู้ดูแลระบบ สถานศึกษาละ จำนวน 1 คน รวม 9 คน

2. ขอบเขตเนื้อหา

2.1 ศึกษาสภาพบริบทขององค์กรเบื้องต้นเพื่อเป็นข้อมูลในการศึกษา

2.2 ศึกษาองค์ประกอบพื้นฐานความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ CIA และนำหัวข้อมาสร้างแบบทดสอบให้สอดคล้องกับบริบทขององค์กร และกำหนดใช้กับกลุ่มเจ้าหน้าที่ทั่วไปในองค์กร

2.3 ศึกษามาตรฐาน ISO 27001:2013 ซึ่งเป็นมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ได้รับการยอมรับในระดับสากล มาสร้างเป็นแบบทดสอบและกำหนดใช้กับกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร

2.4 ศึกษาหลักการวิเคราะห์ความเสี่ยงและเกณฑ์การประเมินความเสี่ยงเพื่อนำมากำหนดใช้ในการสร้างเครื่องมือทดสอบการประเมินฯ

2.5 ศึกษาการออกแบบระบบและสร้างระบบการประเมินเพื่ออำนวยความสะดวกกับผู้ใช้งานและความสะดวกในการจัดเก็บข้อมูล

ประโยชน์ที่คาดว่าจะได้รับ

1. เป็นองค์กรต้นแบบขนาดเล็กที่สามารถพัฒนาเครื่องมือประเมินระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กรได้จากการอ้างอิงมาตรฐานความมั่นคงปลอดภัยและมาตรฐาน ISO 27001:2013 ได้อย่างเหมาะสมกับบริบทขององค์กร
2. องค์กรรับทราบระดับความเสี่ยงและตระหนักในความสำคัญของพฤติกรรมของผู้ใช้งานที่จะนำไปสู่ความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานเทคโนโลยีสารสนเทศในองค์กร
3. ลดค่าใช้จ่ายในการดำเนินการประเมินความเสี่ยงขององค์กร
4. ผู้บริหารองค์กรทราบถึงข้อมูลระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรและหน่วยงานภายในสังกัด และสามารถใช้เป็นข้อมูลประกอบการตัดสินใจในการบริหารจัดการด้านเทคโนโลยีสารสนเทศต่อไป

นิยามศัพท์เฉพาะ

เครื่องมือที่ใช้ในงานวิจัย หมายถึง แบบทดสอบระดับความเสี่ยงฯ แบ่งเป็น 2 ประเภท 1. แบบทดสอบความเสี่ยง ฯ สำหรับเจ้าหน้าที่ทั่วไป 2. แบบทดสอบความเสี่ยง ฯ สำหรับเจ้าหน้าที่ดูแลด้านเทคโนโลยีสารสนเทศในองค์กร

กลุ่มตัวอย่าง หมายถึง เจ้าหน้าที่ทั้ง 2 ประเภท ได้แก่ กลุ่มเจ้าหน้าที่ทั่วไป และกลุ่มเจ้าหน้าที่ดูแลระบบ ในสถาบันการอาชีวศึกษาภาคเหนือ 2

กลุ่มผู้ใช้งาน หมายถึง เจ้าหน้าที่ของสถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 ทั้ง 9 แห่ง ประกอบด้วย ผู้ใช้งานทั่วไป แห่งละ 10 คน รวม 90 คน และเจ้าหน้าที่ดูแลระบบสารสนเทศองค์กร แห่งละ 1 คน รวม 9 คน ดังนั้น กลุ่มผู้ใช้งานจึงมีจำนวนทั้งสิ้น 99 คน

ระดับความเสี่ยง หมายถึง ผลของโอกาส X ผลกระทบ = ระดับความเสี่ยง มี 5 ระดับ ได้แก่

1 = 1–5 เสี่ยงต่ำมาก

2 = 6–10 เสี่ยงต่ำ

3 = 11–15 เสี่ยงปานกลาง

4 = 16–20 เสี่ยงสูง

5 = 21–25 เสี่ยงสูงมาก

องค์ประกอบพื้นฐานความปลอดภัยสารสนเทศ CIA หมายถึง

ความลับ (Confidentiality)

ความคงสภาพ ความครบถ้วน ถูกต้อง (Integrity)

ความพร้อมใช้ (Availability)

มาตรฐาน ISO 27001:2013 หมายถึง มาตรฐานด้านความรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ได้รับการยอมรับตามมาตรฐานสากล

การอ้างอิงมาตรฐานความมั่นคงปลอดภัย หมายถึง การศึกษาหัวข้อหลักของทั้งสองมาตรฐานมาเป็นแนวทางในการสร้างแบบสอบถามให้สอดคล้องกับสภาพบริบทขององค์กร

สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 หมายถึง วิทยาลัยเทคนิคเชียงราย วิทยาลัยอาชีวศึกษาเชียงราย วิทยาลัยเทคนิคกาญจนาภิเษกเชียงราย วิทยาลัยเทคนิคพะเยา วิทยาลัยเกษตรและเทคโนโลยีพะเยา วิทยาลัยเทคนิคแพร่ วิทยาลัยอาชีวศึกษาแพร่ วิทยาลัยเกษตรและเทคโนโลยีแพร่ และวิทยาลัยเทคนิคน่าน

การทดลองสร้างหรือการพัฒนาระบบ หมายถึง การศึกษาข้อมูลและการทดลองสร้างระบบเพื่อใช้ในการประเมินที่ยังไม่ใช่ระบบที่เสร็จสมบูรณ์พร้อมให้ผู้ใช้งานใช้ได้ แต่เป็นเพียงการทดลองในระดับแรก ทดลองใช้กับกลุ่มตัวอย่างเท่านั้น

ระบบ IT RSM หมายถึง (IT Risk assessment) ระบบที่ถูกทดลองสร้างขึ้นเพื่อเป็นเครื่องมือสำหรับการทำแบบประเมินระดับความเสี่ยงผ่านระบบออนไลน์ สามารถรวบรวมและจัดเก็บข้อมูลผู้ใช้งานได้

กรอบการวิจัย

แนวทางในการกำหนดข้อคำถามตามหลักองค์ประกอบความปลอดภัยด้านสารสนเทศพื้นฐาน CIA และมาตรฐานความปลอดภัยระดับสากล ISO27001:2013

–ศึกษาบริบทสภาพทั่วไปและการใช้งานสารสนเทศในองค์กรของกลุ่มตัวอย่าง

–ศึกษามาตรฐานการรักษาความมั่นคงปลอดภัยขั้นพื้นฐาน

–ศึกษามาตรฐาน ISO 27001:2013 ซึ่งเป็นมาตรฐานการยอมรับด้านเทคโนโลยีสารสนเทศระดับสากล

–ศึกษาการกำหนดระดับความเสี่ยง

–ศึกษาเกี่ยวกับการออกแบบการจัดการข้อมูลในระบบ

พฤติกรรมการใช้งานของกลุ่มตัวอย่าง

–เจ้าหน้าที่ทั่วไปในองค์กร

–เจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร

เกณฑ์การกำหนดระดับความเสี่ยง

โอกาส X ความรุนแรงของเหตุการณ์ = ความเสี่ยง

ผลกระทบที่อาจเกิดขึ้นแบ่งเป็น 5 ระดับ

1 = ต่ำมาก 1–5 คะแนน

2 = ต่ำ 6–10 คะแนน

3 = ปานกลาง 11–15 คะแนน

4 = มาก 16–20 คะแนน

5 = มากที่สุด 21–25 คะแนน

บทที่ 2

เอกสารและงานวิจัยที่เกี่ยวข้อง

การศึกษาวิจัย เรื่อง การพัฒนาระบบประเมินความเสี่ยงการใช้เทคโนโลยีสารสนเทศในองค์กรเบื้องต้น ผู้วิจัยได้ทำการศึกษาค้นคว้าเอกสารและงานวิจัยที่เกี่ยวข้อง จำแนกตามหัวข้อลำดับ ดังนี้

มาตรฐานความมั่นคงปลอดพื้นฐานภัยด้านเทคโนโลยีสารสนเทศ CIA

มาตรฐาน ISO 27001: 2013

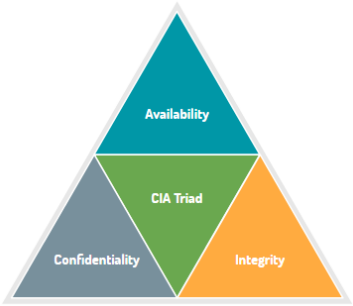
ความเสี่ยงและการประเมินความเสี่ยง

การออกแบบระบบ

งานวิจัยที่เกี่ยวข้อง

มาตรฐานความมั่นคงปลอดพื้นฐานภัยด้านเทคโนโลยีสารสนเทศ CIA Triangle

NSTISSC Nation Security Telecommunications and Information Systems Security คณะกรรมการด้านความมั่นคงด้านโทรคมนาคมและระบบสารสนเทศแห่งชาติของสหรัฐอเมริกา เป็นผู้กำหนดแนวคิดความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขึ้น ซึ่งต่อมาได้รับการยอมรับในระดับสากล โดยได้กล่าวถึงสิ่งสำคัญในการดำเนินงานความมั่นคงปลอดภัยของสารสนเทศนั้น มีสิ่งที่ต้องคำนึงถึงเป็นหลัก ได้แก่ ความลับ Confidentiality ความคงสภาพ Integrity และความพร้อมใช้งาน Availability หรือที่เรียกว่าสามเสาหลักความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ



ภาพ 1 แสดง CIA Triad ในโลกของ Security

ที่มา: บริษัท QA Hive จำกัด, 29 ธันวาคม 2566, Https: //www.Qahive.com

นอกจากนั้นยังคงต้องคำนึงถึงนโยบายการปฏิบัติงาน การให้การศึกษา และเทคโนโลยีที่จะนำมาใช้เป็นกลไกควบคุมและป้องกันที่ต้องเกี่ยวข้องกับการจัดการความมั่นคงปลอดภัย ด้วย มาตรฐานความมั่นคงปลอดภัย CIA ประกอบด้วย

ความลับ Confidentiality เนื่องด้วยข้อมูลบางประเภทมีความจำเป็นอย่างยิ่งที่จะต้องถูกจัดเก็บเป็นความลับ ไม่สามารถเปิดเผยสาธารณะทั่วไปได้ เพราะหากถูกเปิดเผยอาจทำให้เกิดความเสียหายหรือเป็นอันตรายได้ ในการรักษาความลับเป็นการรับประกันให้ผู้มีสิทธิ์และผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ ทั้งนี้องค์กรจึงจำเป็นต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับ โดยการกำหนดนโยบายรักษาความมั่นคงปลอดภัยและนำไปใช้ให้แก่บุคลากรหรือทีมงานความมั่นคงปลอดภัยและผู้ใช้งาน สำหรับกลไกหลักที่ใช้ในการรักษาความลับ คือ การเข้ารหัสข้อมูล Key Password และการพิสูจน์ทราบตัวตน

ความคงสภาพ Integrity คือ ความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลกปลอมเข้าสู่ระบบ สารสนเทศจะขาดความคงสภาพเมื่อสารสนเทศนั้นถูกเปลี่ยนแปลง แก้ไข หรือปลอมปนด้วยสารสนเทศอื่นถูกทำให้เสียหาย ทำลาย หรือกระทำในรูปแบบอื่น ๆ ส่งผลต่อความเชื่อถือของข้อมูลหรือแหล่งที่มา ผู้รับผิดชอบจึงต้องปกป้องข้อมูลให้คงสภาพเดิมไม่ให้ถูกดัดแปลงแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต กลไกหลักที่ใช้ในการรักษาความคงสภาพประกอบด้วย 2 ส่วนคือ Prevention เป็นการป้องกันไม่ให้มีการเปลี่ยนแปลงแก้ไขข้อมูลโดยผู้ที่ไม่ได้รับอนุญาตรวมถึงป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลนอกเหนือขอบเขตของผู้ที่ได้รับอนุญาต ซึ่งอาจใช้การพิสูจน์ตัวตน Authentication และการควบคุมการเข้าถึง และ Detection การตรวจสอบข้อมูลว่ายังคงมีความน่าเชื่อถือได้อยู่หรือไม่ ซึ่งสามารถตรวจเช็ควิเคราะห์เหตุการณ์ต่าง ๆ ที่เกิดขึ้นจาก Log file

ความพร้อมใช้ Availability คือ ความสามารถในการใช้ข้อมูลหรือทรัพยากรเมื่อต้องการเข้าถึงสารสนเทศ โดยการเข้าถึงหรือเรียกใช้งานสามารถดำเนินได้อย่างราบรื่นโดยผู้ใช้หรือระบบอื่นที่ได้รับอนุญาตเท่านั้น หากเป็นผู้ใช้หรือระบบที่ไม่ได้รับอนุญาตการเข้าถึงหรือเรียกใช้งานจะถูกขัดขวางและล้มเหลวในที่สุด ความพร้อมใช้งานจัดเป็นส่วนหนึ่งของความมั่นคง ความน่าเชื่อถือของระบบ โดยที่ระบบอาจถูกโจมตีโดยผู้ไม่ประสงค์ดีที่พยายามทำให้ระบบไม่สามารถใช้งานได้

ดังนั้น ในกรณีที่ข้อมูลอาจได้รับความเสียหาย สูญเสียหรือสารสนเทศขาดคุณสมบัติในด้านใดด้านหนึ่งหรือหลายด้าน จากทั้ง 3 คุณสมบัติข้างต้น ได้แก่ ความลับ ความคงสภาพ และความพร้อมใช้จะถือว่า ข้อมูลหรือสารสนเทศนั้นไม่มีความปลอดภัย นอกเหนือจากที่

มาตรฐานความปลอดภัยขั้นพื้นฐานที่กล่าวมาข้างต้นทั้ง 3 แล้วยังมีมาตรฐานที่กำหนดเพิ่มเติมอีกแต่ในการศึกษาค้นคว้าครั้งนี้ ผู้วิจัยขอนำเสนอข้อมูลเพียง 3 ส่วนที่เกี่ยวข้องและสอดคล้องกับบริบทขององค์กรที่เลือกเป็นกลุ่มตัวอย่างในการศึกษา

มาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ISO 27001 : 2013

ISO 27001 คือ มาตรฐานจัดการความมั่นคงปลอดภัยด้านสารสนเทศชั้นนำในระดับสากล องค์กรทั่วโลกให้การยอมรับ ในการนำไปใช้และยังคงรักษามาตรฐานของระบบจัดการความมั่นคงด้านสารสนเทศ ISO 27001 นี้ไว้เพื่อรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลที่มีความสำคัญยิ่ง ลดความเสี่ยง ไม่ทำให้การทำงานสะดุด เพิ่มความมั่นใจให้ผู้ใช้บริการและผู้มีส่วนได้เสีย

ภาพ 2 แสดงQuality Steams 27001:2013

ที่มา: บริษัท Quality Systems จำกัด, 29 ธันวาคม 2566, https: //www.Qltysys.com.

จุดเริ่มต้นและพัฒนามาจากการพัฒนาความมั่นคงปลอดภัยขั้นพื้นฐาน CIA โดย International Organization for Standardization หรือที่รู้จักกัน ISO และ International Electrotechnical Commission หรือ IEC ซึ่งเป็นมาตรฐานระบุข้อกำหนดสำหรับการดำเนินการและการบริหารจัดการ Information Security Management Systems: ISMS ที่มีประสิทธิภาพเพื่อป้องกันสาเหตุของความเสี่ยงด้านความปลอดภัยข้อมูล ISO 27001 ประกาศใช้ครั้งแรกเมื่อปี 2550 เวอร์ชั่นปัจจุบัน คือ ISO 27001:2013 ถูกพัฒนามาจากเวอร์ชั่น 27001:2005 ประกาศใช้เมื่อวันที่ 1 ตุลาคม 2556 ได้มีการใช้ระยะเวลาในการทบทวนพัฒนานานและช้ากว่ากำหนดที่ได้มีการกำหนดไว้ทุก ๆ 5 ปีในการพัฒนาปรับเปลี่ยนเวอร์ชั่นการใช้งาน โดยเวอร์ชั่นปัจจุบันใช้ระยะเวลา 8 ปี ในการปรับเปลี่ยน เนื่องด้วยการเปลี่ยนแปลงของโลกเทคโนโลยีที่มีการเปลี่ยนแปลงรูปแบบโฉมการใช้งานอุปกรณ์ไอทีทั้งในระดับบุคคลและระดับองค์กร จึงเป็นเหตุ

สำคัญทำให้เกิดบทบาทของเทคโนโลยี virtual และคลาวด์ (cloud) ขึ้น บวกกับการปรับโครงสร้างมาตรฐาน Annex SL ซึ่งเป็นรูปแบบเอกสารสำหรับมาตรฐานการจัดการ ISO ทุกตัว เพื่อให้โครงสร้าง คำจำกัดความและนิยามของมาตรฐานต่าง ๆ ในระบบบริหารจัดการที่เป็น ISO เป็นไปในทิศทางเดียวกัน อีกทั้งสนับสนุนให้องค์การที่มีการทำระบบบริหารจัดการ management system มากกว่าหนึ่งมาตรฐานสามารถควบรวมและทำงานประสานกันได้เป็นอย่างดียิ่งขึ้น ซึ่งในโครงสร้างมีข้อกำหนดทั้งหมด 10 ข้อจากเดิม 8 ข้อ เปลี่ยนโครงสร้างจาก 11 โดเมน เป็น 14 โดเมน ลด control ลง จาก 133 เป็น 114 ข้อ และได้มีการประยุกต์ใช้หลักการ Plan–Do–Check–Act (PDCA) เข้ามาจัดการข้อมูลให้เป็นไปอย่างมีระบบ มีการบริหารจัดการเชิงกระบวนการที่ใช้กันอย่างแพร่หลาย มุ่งเน้นการวางแผนก่อนลงมือปฏิบัติงาน การจัดทำนโยบาย การลงมือทำอย่างรอบคอบรัดกุม รวมถึงมีการควบคุม ตรวจสอบและประเมินความเสี่ยงในการปฏิบัติงานอยู่เสมอ

ISO/IEC 27001 เป็นมาตรฐานที่ระบุข้อกำหนดในการดำเนินการและการบริหารจัดการ ISMS ที่มีประสิทธิภาพเพื่อป้องกันสาเหตุของความเสี่ยงด้านความปลอดภัยข้อมูล สำหรับองค์กรที่ได้รับการรับรองมาตรฐาน ISO/IEC 27001 จะช่วยเสริมสร้างความสามารถในการป้องกันตนเองจากการโจมตีทางไซเบอร์ ช่วยป้องกันการเข้าถึงข้อมูลที่สำคัญและละเอียดอ่อนหรือเป็นความลับได้ ในเบื้องต้นขอบเขตของมาตรฐาน ISO/IEC 27001 มีวัตถุประสงค์เพื่อครอบคลุมข้อมูลทุกประเภท โดยไม่คำนึงถึงรูปแบบองค์กร และในปี 2568 องค์กรที่มีการรับรองมาตรฐาน ISO 27001:2013 จะต้องทำการปรับปรุงไปใช้ในเวอร์ชั่น 27001:2022 ภายในวันที่ 31 มีนาคม 2568 นี้ แต่ปัจจุบันยังคงต้องใช้ มาตรฐาน ISO 27001:2013 อยู่ก่อน สำหรับ มาตรฐาน ISO 27001:2013 ประกอบด้วย 14 หมวดหัวข้อหลัก ดังนี้ 1) นโยบายความมั่นคงปลอดภัยสารสนเทศ 2) โครงสร้างความมั่นคงปลอดภัยสารสนเทศ 3) ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล 4) การบริหารจัดการทรัพย์สิน 5) การควบคุมการเข้าถึง 6) การเข้ารหัสข้อมูล 7) ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม 8) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน 9) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล 10) การจัดหา พัฒนา และการบำรุงรักษาระบบ 11) ความสัมพันธ์กับผู้ให้บริการภายนอก 12) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ 13) ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ 14) ความสอดคล้อง

ความเสี่ยงและการประเมินความเสี่ยง

ความเสี่ยง Risk คือ โอกาส สาเหตุหรือปัจจัยที่จะทำให้เกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเสีย หรือเหตุการณ์ที่ไม่พึงประสงค์ การกระทำใด ๆ ที่อาจจะเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอนแบบไม่ทันระวัง ซึ่งอาจจะเกิดขึ้นในอนาคตส่งผลกระทบต่อการดำเนินงานไม่เป็นไม่ตามวัตถุประสงค์ หรือไม่สามารถนำไปสู่เป้าหมายความสำเร็จขององค์กรที่วางไว้ได้

การประเมินความเสี่ยง Risk Assessment คือ กระบวนการระบุ วิเคราะห์และการจัดลำดับความเสี่ยงโดยการประเมินจากโอกาสที่จะเกิดและผลกระทบ เมื่อทำการประเมินแล้วทำให้ทราบถึงระดับของความเสี่ยง แบ่งออกเป็น 5 ระดับ ได้แก่ สูงมาก สูง ปานกลาง น้อย และน้อยมาก

แผนผังประเมินความเสี่ยง (Risk Assessment Matrix)

Risk Assessment Matrix			ความเป็นไปได้				
			ต่ำมาก / น้อยมาก	ต่ำ / น้อย	ปานกลาง	สูง / บ่อย	สูงมาก / บ่อยมาก
			1	2	3	4	5
ผลกระทบ / ความรุนแรง	สูงมาก / หายนะ	5	5	10	15	20	25
	สูง / วิกฤต	4	4	8	12	16	20
	ปานกลาง	3	3	6	9	12	15
	ต่ำ / น้อย	2	2	4	6	8	10
	ไม่เป็นสาระสำคัญ / น้อยมาก	1	1	2	3	4	5
			ระดับของความเสี่ยง				

ภาพ 3 แสดงผังการประเมินระดับความเสี่ยง

ที่มา: พันธุ์ทอง จันทร์สว่าง, PT NEWS, https://ptjsw.blogspot.com/2017/12/8-2560-eocsat-10-risk-likelihood-x.html

การบริหารความเสี่ยง Risk Management คือ กระบวนการดำเนินงานที่เป็นระบบและต่อเนื่องขององค์กร เพื่อลดสาเหตุที่จะนำไปสู่ความเสียหายในแต่ละระดับ ที่อาจจะเกิดขึ้นในอนาคต โดยการคำนึงถึงการบรรลุความสำเร็จตามวัตถุประสงค์หรือเป้าหมายขององค์กรเป็นหลัก

การควบคุม Control คือ นโยบาย แนวทางหรือขั้นตอนการปฏิบัติต่าง ๆ ในการลดความเสี่ยง แบ่งได้ 4 ประเภท ได้แก่ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO Committee of Sponsoring Organization of the Tread way Commission ได้แก่ การกำหนดเป้าหมายการบริหารความเสี่ยง การระบุความเสี่ยงต่าง ๆการประเมินความเสี่ยง กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง กิจกรรมการบริหารความเสี่ยง

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร คือ กระบวนการทำงานที่ช่วยให้ IT Managers สามารถสร้างความสมดุลและดำเนินการระหว่างมาตรการในการป้องกันและบรรลุความสำเร็จ ด้วยการปกป้องระบบเทคโนโลยีสารสนเทศและข้อมูลสำคัญ ซึ่งจะช่วยสนับสนุนความสำเร็จของการบรรลุพันธกิจขององค์กร

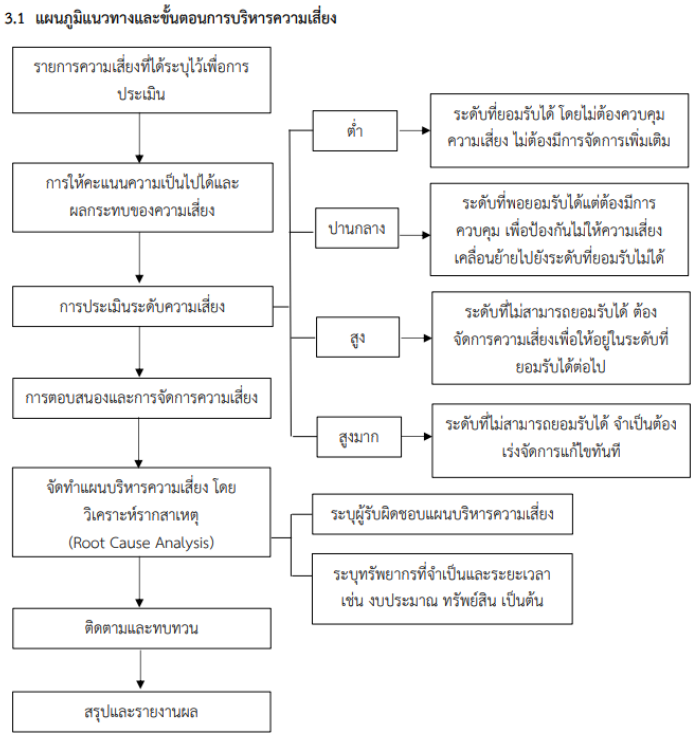
Access Risk คือ ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ อาจเกิดได้จากหลายสาเหตุ ได้แก่ การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นในการใช้งาน การไม่ได้กำหนดรหัสผ่าน ในการเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ การไม่ได้จำกัดและควบคุมให้เฉพาะเจ้าหน้าที่ที่มีสิทธิ์หรืออำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์ เป็นต้น

Integrity Risk คือ ความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลการทำงานของระบบคอมพิวเตอร์ที่อาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีสิทธิ์หรือหน้าที่ที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด อาจมีสาเหตุมาจากหน่วยงานไม่มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีสิทธิ์ อำนาจหน้าที่ ที่เกี่ยวข้อง รัดกุมเพียงพอ ทำให้ข้อมูล และการทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลงไปได้

Availability Risk คือ ความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ อาจทำให้การปฏิบัติงานหยุดชะงักได้ ความเสี่ยงนี้อาจเกิดได้จากการที่ไม่ได้ควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และมีการป้องกันความเสียหายอย่างเพียงพอ รวมไปถึงการไม่มีการสำรองข้อมูล และระบบงานคอมพิวเตอร์และจัดให้มีแผนสำรองกรณีเกิดเหตุการณ์ฉุกเฉิน

Infrastructure Risk คือ ความเสี่ยงเกี่ยวกับการที่หน่วยงานองค์กรไม่มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดีจัดให้มีระบบคอมพิวเตอร์และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการดำเนินงาน ความเสี่ยงนี้อาจเกิดจาก องค์กรขาดระบบการสอบยันและการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการไม่มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่าง ๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน

นอกจากความเสี่ยง ดังกล่าวข้างต้นนี้ ยังมีความเสี่ยงเกี่ยวกับการที่ผู้บริหารของหน่วยงานองค์กรที่ไม่มีการรับข้อมูลที่เกี่ยวข้องอย่างถูกต้องและทันเวลาเพื่อใช้ประกอบการตัดสินใจ ดังนั้น หน่วยงานควรพิจารณาว่าข้อมูลใดบ้างที่จำเป็นแก่การตัดสินใจ รวมทั้งจัดให้มีระบบการตรวจสอบความถูกต้องของข้อมูล การจัดเตรียมข้อมูลให้พร้อมเพื่อประโยชน์ในการดำเนินงานของหน่วยงานองค์กรต่อไป



ภาพ 4 แสดงตัวอย่างแผนภูมิแนวทางการบริหารความเสี่ยง

ที่มา: งานเทคโนโลยีสารสนเทศ คณะแพทย์ศาสตร์ มหาวิทยาลัยเชียงใหม่, 2566, https: //w2.med.cmu.ac.th

การบริหารความเสี่ยงตามมาตรฐาน COSO

ประกอบด้วยองค์ประกอบ 8 ประการซึ่งครอบคลุมแนวทางการกำหนดนโยบายการบริหารงาน การดำเนินงาน และการบริหารความเสี่ยง ดังนี้

1) สภาพแวดล้อมภายในองค์กร (Internal Environment)

2) การกำหนดวัตถุประสงค์ (Objective Setting)

3) การบ่งชี้เหตุการณ์ (Event Identification)

4) การประเมินความเสี่ยง (Risk Assessment)

5) การตอบสนองความเสี่ยง (Risk Response)

6) กิจกรรมการควบคุม (Control Activities)

7) สารสนเทศและการสื่อสาร (Information and Communication)

8) การติดตามประเมินผล (Monitoring)

การพัฒนาและออกแบบระบบการใช้งาน

การออกแบบระบบ System Design คือ กระบวนการวางแผนระบบใหม่ หรือระบบที่จะนำมาเสริมกับระบบเดิมที่มีอยู่แล้ว จุดประสงค์ของการออกแบบระบบคือ ตัดสินว่าจะสร้างระบบอย่างไร จึงจะสอดคล้องกับเอกสารความต้องการ การออกแบบทั้งระบบจะประกอบด้วย การออกจอภาพบันทึกข้อมูล การออกแบบรายงานและส่วนแสดงผลอื่น ๆ การออกแบบแฟ้มข้อมูล ฐานข้อมูล รวมทั้งการออกแบบการควบคุมภายในและภายนอกเมื่อออกแบบเสร็จเรียบร้อยแล้วจะต้องจัดทำเอกสารประกอบการออกแบบ เอกสารนี้ เรียกว่า คุณลักษณะเฉพาะของระบบ System Specification

การพัฒนาระบบ System Development การพัฒนาระบบ คือ ขั้นตอนที่สร้างระบบจริง ๆ ในขั้นนี้จะมีการเขียนโปรแกรม ทดสอบโปรแกรมและเขียนคู่มือการใช้ระบบ ผลการทำงานในขั้นนี้ คือ โปรแกรมประยุกต์และคู่มือการใช้โปรแกรม

การนำไปใช้และการประเมินผล System Implementation and Evaluation หลังจากการพัฒนาระบบเสร็จเรียบร้อยแล้วก็ถึงขั้นการนำไปใช้งานจริง กิจกรรมในขั้นนี้ประกอบด้วย การแปลงแฟ้มข้อมูลจากระบบเก่าสู่ระบบใหม่การฝึกอบรมผู้ใช้ และการถ่ายโอนจากระบบเก่าไปสู่ระบบใหม่ ณ จุดนี้คือ จุดที่ผู้ใช้และผู้บริหารเริ่มใช้ระบบใหม่จริงหลังจากใช้ระบบไปสักระยะหนึ่งจะต้องจัดให้มีการประเมินระบบจุดมุ่งหมายของการประเมินก็เพื่อตรวจสอบว่าระบบทำงานได้จริงตามที่เจอหรือไม่

งานวิจัยที่เกี่ยวข้อง

ชนกานต์ อาภรณ์พงษ์ และบัวเรียน สูงพล ได้ศึกษากรอบโครงร่างความมั่นคงปลอดภัยระบบสารสนเทศ (ISO27001:2013) กรณีศึกษา สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ จากการศึกษาเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. กับมาตรฐาน ISO27001 มีวัตถุประสงค์ให้องค์กรในภาคตลาดทุน หรือตลาดหลักทรัพย์เกิดประสิทธิภาพในการปฏิบัติ รักษา ปรับปรุงและพัฒนาระบบบริหารความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศอย่างต่อเนื่องและสร้างความมั่นใจได้ถึงแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ตจัดให้มีแนวทางในการแนะนำองค์กรหรือหน่วยงานในภาคตลาดทุนให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศตามมาตรฐานสากลที่พัฒนาขึ้นโดย ISO ผลการทำแบบประเมินความพึงพอใจเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. กับมาตรฐาน ISO27001 พบว่า ผลการแปลผลการตอบแบบประเมิน

ความพึงพอใจการเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต.กับมาตรฐานISO 27001 โดยรวมอยู่ในระดับมีความพึงพอใจมาก สอดคล้องกับการวิเคราะห์เนื้อหาของสารสนเทศโดยเนื้อหาของแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. ครอบคลุมตามมาตรฐาน ISO 27001 และสามารถปรับปรุงเนื้อหาเพิ่มเติมเพื่อให้ครบถ้วนตามมาตรฐาน ISO27001 ได้

จิระ จิตสุภา ปรัชญนันท์ นิลสุข และ พัลลภ พิริยะสุรวงศ์ ได้ศึกษาการสังเคราะห์เนื้อหาความมั่นคง ปลอดภัยทางเทคโนโลยีสารสนเทศ ตามมาตรฐานสากลที่อยู่บนพื้นฐานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ ยึดกรอบดำเนินการที่เป็นสากล ประกอบด้วย การเก็บรักษาข้อมูลไว้เป็นความลับ Confidentiality ความสมบูรณ์ของข้อมูล Integrity และความพร้อมใช้ของข้อมูล Availability ทั้งหมดรวมเรียกว่า CIA โดยได้ทำการเลือกเอามาตรฐานการดำเนินงานที่มีมาตรฐานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศทั้ง 7 มาตรฐานที่ได้รับการยอมรับ ได้แก่ มาตรฐาน ISO 27001: 2005 มาตรฐาน ITIL มาตรฐาน FIPS PUB 200 มาตรฐาน NIST800 – 14 มาตรฐาน IT BPM มาตรฐาน COBIT และมาตรฐาน COSO โดย ผ่านการสังเคราะห์และเปรียบเทียบแนวทางปฏิบัติของมาตรฐานสากล 7 มาตรฐาน ได้แนวทางปฏิบัติ 10 แนวทางผลการศึกษา พบว่า แต่ละมาตรฐานมีแนวทางการปฏิบัติเพื่อความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่ไม่เหมือนกัน เนื่องจากการให้ความสำคัญและจุดเน้นด้านความมั่นคงปลอดภัยที่แตกต่างกันออกไป แต่มาตรฐานที่ได้รับการยอมรับและ มีแนวทางการปฏิบัติครบทั้ง 10 แนวทาง ได้แก่ มาตรฐาน ISO 27001 เป็นมาตรฐานที่มีแนวทางปฏิบัติครบทั้ง 10 แนวทาง เป็นมาตรฐานที่ได้รับการยอมรับและนำไปใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในองค์กรทั่วโลก ในขณะที่มาตรฐานอื่นๆมีแนวทางการปฏิบัติที่ไม่ครบทั้ง 10 แนวทางตามลำดับ ให้สอดคล้องกับการศึกษาของผู้วิจัยที่ได้นำเอา มาตรฐาน ISO 27001 มาเป็นแนวทางในการสร้างเครื่องมือประเมินความเสี่ยงการใช้งานสารสนเทศในองค์กร

ชุลีกร นวลสมศรี และ ดร.สุทธิศักดิ์ จันทรวงษ์โส ได้ศึกษาการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO 27001:2013 กรณีศึกษาขององค์กรด้านการบินแห่งหนึ่ง โดยนำเอามาตรฐานการประเมิน ทั้ง 14 หัวข้อ ตามมาตรฐาน ISO 27001:2013 พบว่า องค์กรกรณีศึกษามีความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับสูงมี 6 ด้าน ได้แก่ (1) นโยบายความมั่นคงปลอดภัยสารสนเทศ (2) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (3) ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (4) ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (5) ความมั่นคง

ปลอดภัยทางกายภาพและสิ่งแวดล้อม และ (6) การบริการจัดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ทำให้การวิจัยนี้ส่งผลให้องค์กรมีแนวทางในการกำหนดนโยบายและแนวทางในการนำไปใช้ในการบริหารความเสี่ยงทั้ง 6 ด้าน ได้อย่างเหมาะสม

Dhoha Almubayedh and Mashael Al khalis พร้อมด้วยคณะ ได้ศึกษาปัญหาที่เกี่ยวข้องกับความปลอดภัยข้อมูลขององค์กรธุรกิจขนาดเล็ก กรณีศึกษาองค์กรในซาอุดิอาระเบีย พบว่าปัญหาที่นำมาซึ่งการเกิดอาชญากรรมทางไซเบอร์ที่พบในองค์กรขนาดเล็กในซาอุดิอาระเบียส่วนใหญ่เกิดขึ้นจาก องค์กรไม่มีนโยบายในการรักษาความปลอดภัยของข้อมูลซึ่งองค์กรขนาดเล็กในซาอุดิอาระเบียส่วนใหญ่ใช้ระบบอินเตอร์เน็ตในการประกอบธุรกิจจึงทำให้องค์กรขนาดเล็กเป็นเป้าหมายและง่ายในการถูกโจมตีความลับข้อมูลขององค์กร รองลงมาคือ พนักงานในองค์กรขาดความตระหนักรู้ในการรักษาความปลอดภัยของข้อมูลในองค์กรและขาดความรู้ความเข้าในการรักษาข้อมูลความลับขององค์กร รองลงมาคือ องค์กรขาดการควบคุมหรือการทำสัญญาในเรื่องการรักษาความลับกับหน่วยงานหรือองค์กรภายนอกที่ว่าจ้างให้ดำเนินกิจการด้านเว็บไซต์ให้กับองค์กรธุรกิจ จากการสรุปผลการศึกษาองค์กรกรณีศึกษาขาดการควบคุมมาตรฐานความปลอดภัยเบื้องต้นด้านเทคโนโลยีสารสนเทศ CIA และควรมีการควบคุมโดยนำมาตรฐานความปลอดภัยด้านสารสนเทศ ISO 27001 เข้ามาตรวจสอบและใช้เป็นแนวทางในการดำเนินธุรกิจเพื่อป้องกันไม่ให้เกิดความเสียหายในองค์กรขนาดเล็กและสิ่งสำคัญคือองค์กรต้องมีการกำหนดนโยบายการดำเนินงานที่ชัดเจนและสร้างความเข้าใจให้แก่บุคลากรในองค์กร สอดคล้องในการวิจัยที่องค์กรขนาดเล็กเองก็ควรมีนโยบายและมาตรการกำหนดเรื่องการรักษาความปลอดภัยข้อมูลในองค์กร ซึ่งในการประเมินมีข้อคำถามที่ประเมินองค์กรไว้ในแบบทดสอบแล้ว

ณัฐนันท์ พรทวีวัฒน์ และชัยพร เขมะภาตะพันธ์ ได้ประยุกต์ใช้มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ ISO 27001:2013 ซึ่งประกอบด้วย 14 ข้อหลัก และ 35วัตถุประสงค์ 114 มาตรการ มาเป็นแนวทางในการประเมินความเสี่ยงบริษัท อาร์ วีซี คอนสตั๊คชั่น จำกัด และหาแนวทางแก้ไขความเสี่ยงโดยการจัดทำแผนการบริหารจัดการความเสี่ยง และเมื่อได้ดำเนินการประเมินความเสี่ยงก่อนการบริหารจัดการความเสี่ยงแล้วนั้นได้ดำเนินการประมวลผล สรุปผลและหาแนวทางการแก้ไข ซึ่งช่วยลดผลกระทบที่อาจเกิดขึ้น และสามารถบริหารความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ อีกทั้งช่วยลดผลกระทบที่อาจเกิดขึ้นในอนาคตได้ อีกทั้งยังเป็นการเพิ่มประสิทธิภาพในการทำงานของระบบเทคโนโลยีสารสนเทศภายในองค์กรให้มีมาตรฐานเพิ่มมากขึ้นด้วย จากการศึกษามีความสอดคล้องกับงานวิจัยที่มีการประยุกต์ใช้มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ ISO27001:2013

ซึ่งประกอบด้วย 14 ข้อหลัก และ 35 วัตถุประสงค์ มาเป็นแนวทางในการกำหนดเป็นแนวทางการประเมินความเสี่ยงในองค์กร

อรวรรณ ดีลาเกียรติวณิช ได้ศึกษาเกี่ยวกับปัจจัยที่มีผลต่อการบริหารความเสี่ยง กรณีศึกษา: มหาวิทยาลัยราชภัฏธนบุรี จากการเก็บข้อมูลจากอาจารย์และเจ้าหน้าที่ในมหาวิทยาลัย วิเคราะห์ทางสถิติการศึกษาด้วยค่าร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน ทำการทดสอบวิเคราะห์ค่าสัมประสิทธิ์สหสัมพันธ์เพียร์สัน และวิเคราะห์การแปรปรวนทางเดียว กับกลุ่มตัวอย่าง จำนวน 220 คนปัจจัยที่มีอิทธิพลต่อองค์ประกอบการบริหารความเสี่ยง คือ การวางแผน จากการศึกษาทำให้ทราบถึง ประโยชน์ของการบริหารความเสี่ยงที่มีประสิทธิภาพควรมีคำนึงถึงปัจจัยภายในและภายนอก โดยเฉพาะด้านการบริหารที่จะมีส่วนช่วยให้องประกอบการบริหารความเสี่ยงประสบความสำเร็จยิ่งขึ้น

สมหทัย จารุพิมล และนภสินธุ์ บุญมาก ได้ศึกษาเกี่ยวกับ องค์กรกับการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ พบการศึกษาได้มีการนำเอาองค์ประกอบความมั่นคงปลอดภัยขั้นพื้นฐาน CIA มาใช้ในการศึกษางานวิจัย พบว่า องค์กรกรณีศึกษาจะต้องมีการประเมินความเสี่ยงในด้านการเข้าถึงข้อมูลสารสนเทศ, ความถูกต้อง ความครบถ้วนของข้อมูลสารสนเทศ, ความพร้อมใช้ของข้อมูลสารสนเทศและการบริหารจัดการด้านเทคโนโลยีสารสนเทศ รวมถึงการประเมินความเสี่ยงด้านอื่น ๆ ที่เกี่ยวข้องและมีผลกระทบต่อการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศทั้งทางตรงและทางอ้อม ซึ่งมีขั้นตอนในการบริหารความเสี่ยงครบทั้ง 6 ขั้นตอนจะช่วยปกป้องให้สินทรัพย์ขององค์กรมีความปลอดภัย ทั้งนี้ การดำเนินการองค์กรกรณีศึกษาจะต้องให้ความสำคัญและมอบหมายให้ผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศเป็นผู้ดำเนินการ และฝ่ายบริหารขององค์กรให้การสนับสนุนทรัพยากรที่จำเป็น เหมาะสมและได้มาตรฐาน ตลอดจนการสื่อสารภายในองค์กร และสร้างความตระหนักเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ และการใช้งานข้อมูลสารสนเทศให้กับบุคลากรทุกระดับภายในองค์กรด้วย

บทที่ 3

วิธีดำเนินการวิจัย

งานวิจัยนี้เป็นการศึกษาระดับความเสี่ยง และพัฒนาเครื่องมือประเมินระดับความเสี่ยงจากใช้งานเทคโนโลยีสารสนเทศในองค์กรโดยการอ้างอิงมาตรฐานความปลอดภัยด้านเทคโนโลยีสารสนเทศขั้นพื้นฐาน CIA และมาตรฐานความปลอดภัยด้านเทคโนโลยีสารสนเทศที่ได้รับการยอมรับระดับสากล ISO 27001:2013 เพื่อนำไปตรวจสอบและวัดระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศของบุคลากรในองค์กร กรณีศึกษา สถาบันการอาชีวศึกษาภาคเหนือ 2 ซึ่งเป็นองค์กรขนาดเล็กที่ไม่มีการจำทำหรือสร้างนโนบายเกี่ยวกับด้านการใช้งานเทคโนโลยีสารสนเทศในองค์กรได้ จากการศึกษาบริบทเบื้องต้น จึงทำให้ผู้ศึกษามีความสนใจอยากวัดระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กรขึ้น จึงมีแนวความคิดที่จะศึกษาเกี่ยวกับการแบ่งระดับความเสี่ยง และมาตรฐานความปลอดภัยด้านเทคโนโลยีสารสนเทศขึ้นและได้ทำการทดลองสร้างระบบการประเมินขึ้นมาเพื่อรองรับการใช้งานในการตอบแบบสอบถามที่ถูกสร้างเป็นเครื่องมือ และเพื่อให้ได้ค่าความเที่ยงตรงของแบบสอบถามผู้ศึกษาจึงได้ให้เชี่ยวชาญ จำนวน 3 ท่าน ตรวจสอบหาค่าความเที่ยงตรงของชุดแบบสอบถามที่แบ่งออกเป็น 2 กลุ่ม ได้แก่ กลุ่มเจ้าหน้าที่ทั่วไปในองค์กร และเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร โดยการกำหนดให้กลุ่มผู้ใช้งานทั่วไปใช้ชุดแบบสอบถามจากการอ้างอิงข้อมูล มาตรฐานความปลอดภัย CIA และผู้ดูแลระบบสารสนเทศองค์กรใช้มาตรฐาน ISO 20071:2013 มีหัวข้อหลัก 14 หัวข้อ เป็นเกณฑ์กำหนดในการสร้างแบบทดสอบ จากนั้นได้ทำการออกแบบระบบเพื่อให้ข้อมูลยังสามารถอยู่ได้และสามารถเป็นข้อมูลประกอบการตัดสินใจให้กับผู้บริหารองค์กรในการพัฒนาด้านเทคโนโลยีสารสนเทศ โดยผู้วิจัยได้ดำเนินการตามขั้นตอน ดังนี้

การกำหนดขอบเขตการวิจัย

1. เนื้อหาที่ใช้ในการวิจัย ประกอบด้วย

1.1 ศึกษาสภาพบริบทขององค์กรเบื้องต้นเพื่อเป็นข้อมูลในการศึกษา

1.2 องค์ประกอบความมั่นคงปลอดภัยสารสนเทศพื้นฐาน CIA ได้แก่ การรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability)

1.3 มาตรฐาน ISO 27001:2013 มาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยข้อมูล (Information Security Management System: ISMS)

1.4 หลักการวิเคราะห์ความเสี่ยง และเกณฑ์การประเมินความเสี่ยง

1.5 หลักการออกแบบระบบและสร้างระบบการประเมินเพื่ออำนวยความสะดวกกับผู้ใช้งานและควรสามสะดวกในการจัดเก็บข้อมูล

2. ประชากรและกลุ่มตัวอย่าง

การศึกษานี้ เลือกกลุ่มตัวอย่างที่ใช้ คือ กลุ่มเจ้าหน้าที่ทั่วไป ได้แก่ บุคลากรที่ปฏิบัติงานในสถาบันการอาชีวศึกษาภาคเหนือ 2 จำนวน 11 คน โดยแบ่งออกเป็นกลุ่มผู้ใช้งานทั่วไป จำนวน 10 คน และกลุ่มเจ้าหน้าที่ไอที ได้แก่ บุคลากรที่มีหน้าที่ดูแลเทคโนโลยีสารสนเทศในองค์กร จำนวน 1 คน ซึ่งได้มาจากการเลือกกลุ่มตัวอย่างที่ไม่ใช้หลักความน่าจะเป็น(Non–Probability Sampling) อันได้แก่ การเลือกกลุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) และกลุ่มผู้ใช้งาน จำนวน 99 คน ได้แก่ บุคลากรที่ปฏิบัติงานในสถานศึกษาสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 แบ่งเป็น กลุ่มผู้ใช้งานทั่วไป จำนวน 9 แห่งๆ ละ 10 คน รวม 90 คนและกลุ่มเจ้าหน้าที่ไอที จำนวน 9 แห่งๆ ละ 1 คน รวม 9 คน

การกำหนดเครื่องมือที่ใช้ในการวิจัย

การศึกษางานวิจัยนี้ กำหนดให้กลุ่มตัวอย่างได้ทำการประเมินระดับความเสี่ยง ฯ ผ่านทางระบบ IT RSM เพื่อทดสอบระบบ หากพบว่า ระบบยังไม่มีความสมบูรณ์หรือเป็นไปตามที่ต้องการ ระบบจะยังไม่ถูกใช้สำหรับกลุ่มผู้ใช้งาน แต่เป็นการแสดงผลการทดสอบของกลุ่มตัวอย่างเท่านั้น

1. เนื้อหาของแบบทดสอบข้อมูลทั่วไปเกี่ยวกับการใช้งานสารสนเทศในองค์กรที่ได้มาจากองค์ความรู้มาตรฐานความปลอดภัย CIA และมาตรฐาน ISO 27001:2013 มีรายละเอียดดังนี้

1.1 เจ้าหน้าที่ผู้ใช้งานทั่วไป ประกอบด้วย 2 ตอน

ตอนที่ 1 ข้อมูลทั่วไปสำหรับผู้ตอบแบบทดสอบ จำนวน 6 ข้อ

ตอนที่ 2 ข้อมูลแบบทดสอบฯ อ้างอิงจากมาตรฐาน CIA จำนวน 27 ข้อ

1.2 เจ้าหน้าที่ผู้ดูแลระบบ ประกอบด้วย 2

ตอนที่ 1 ข้อมูลทั่วไปสำหรับผู้ตอบแบบทดสอบ จำนวน 5 ข้อ

ตอนที่ 2 ข้อมูลแบบทดสอบฯ อ้างอิงตามมาตรฐาน ISO 27001:2013 จำนวน 67 ข้อ

ทั้งนี้ เมื่อได้รายละเอียดต่าง ๆ ของเนื้อหาทั้ง 1.1 และ 1.2 แล้วจะนำไปบรรจุไว้ในระบบประเมิน IT RSM เพื่อให้กลุ่มตัวอย่างได้ทำการทดสอบเพื่อหาค่าความพึงพอใจ

การใช้งานก่อน เมื่อระบบมีสัดส่วนความพึงพอใจเป็นไปตามความต้องการของผู้วิจัยแล้ว ระบบจะถูกนำไปใช้กับกลุ่มผู้ใช้งานต่อไป

2. ระบบประเมิน IT RSM ประกอบด้วย 4 ส่วน ดังนี้

ส่วนที่ 1 หน้าเข้าสู่ระบบ เป็นหน้าที่ผู้ใช้งานทั่วไปและผู้ดูแลระบบ จะต้องทำการ Log in หรือลงทะเบียนก่อนการเข้าใช้งาน

ส่วนที่ 2 หน้าทำแบบประเมิน โดยจะแบ่งเป็นหน้าของผู้ใช้งานทั่วไปและผู้ดูแลระบบเข้าทำแบบทดสอบเฉพาะกลุ่มของตนเอง ซึ่งข้อมูลของแบบทดสอบเป็นข้อมูลที่ได้มาจากข้อ 1.1 และ 1.2

ส่วนที่ 3 หน้าแสดงผลการประเมิน หลังจากผู้ตอบแบบทดสอบเสร็จสิ้นจะแสดงผลที่ได้จากการทดสอบเฉพาะของตนเอง

ส่วนที่ 4 หน้าแสดงคำแนะนำ จะแสดงแนวทางปฏิบัติในการใช้งานเทคโนโลยีสารสนเทศขององค์กรให้มีความปลอดภัย

การสร้างและหาคุณภาพเครื่องมือ

1. การสร้างแบบทดสอบ

1.1 ศึกษาบริบท สภาพแวดล้อมการปฏิบัติงาน นโยบายผู้บริหาร และแผนการดำเนินงานของสถาบันการอาชีวศึกษาภาคเหนือ 2

1.2 ศึกษาองค์ประกอบมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ CIA ได้แก่ การรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) และที่เกี่ยวข้อง

1.3 ศึกษามาตรฐาน ISO 27001:2013 มาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่ได้รับการยอมรับระดับมาตรฐานสากล (Information Security Management System: ISMS)

1.4 ศึกษาแนวคิดการบริหารจัดการความเสี่ยงของ COSO 2017 (The Committee of Sponsoring Organizations of the Tread Way Commission, 2017)

1.5 ศึกษางานวิจัยที่เกี่ยวข้องกับความเสี่ยงของการใช้เทคโนโลยีสารสนเทศในองค์กร

1.6 ออกแบบและกำหนดข้อคำถามในแบบทดสอบข้อมูลทั่วไปเกี่ยวกับการใช้งานสารสนเทศในองค์กร ซึ่งแบ่งออกเป็นผู้ใช้งานทั่วไปและผู้ดูแลระบบตามองค์ประกอบมาตรฐานความปลอดภัยสารสนเทศ CIA และมาตรฐาน ISO 27001:2013

1.7 นำแบบทดสอบข้อมูลทั่วไปฯ ที่สร้างขึ้นไปให้ผู้เชี่ยวชาญประเมินคุณภาพความถูกต้องตามโครงสร้างเนื้อหาขององค์ประกอบมาตรฐานความปลอดภัยสารสนเทศ CIA และมาตรฐาน ISO 27001:2013 และหลักวิชาการในการจัดทำแบบทดสอบแล้วนำมาปรับปรุงแก้ไขข้อบกพร่องตามข้อเสนอแนะของผู้เชี่ยวชาญ

1.8 นำแบบทดสอบข้อมูลทั่วไปฯ ที่ปรับปรุงแก้ไขแล้วให้ผู้เชี่ยวชาญชุดเดิมทำการประเมินความสอดคล้องของข้อคำถามกับวัตถุประสงค์ในการวิจัยระดับความเสี่ยงการใช้เทคโนโลยีสารสนเทศในองค์กร พร้อมทั้งขอรับข้อแนะนำเพิ่มเติม

1.9 นำคะแนนที่ได้จากการประเมินแบบทดสอบข้อมูลทั่วไปฯ ของผู้เชี่ยวชาญทั้ง 3 ท่าน มาหาดัชนีความสอดคล้องตามเกณฑ์การให้คะแนน +1 เมื่อแน่ใจว่าข้อคำถามนั้นวัดผลได้ตามวัตถุประสงค์ที่กำหนด ให้คะแนน 0 เมื่อไม่แน่ใจว่าข้อคำถามนั้นวัดผลได้ตามวัตถุประสงค์ที่กำหนด และให้คะแนน –1 เมื่อแน่ใจว่าข้อคำถามนั้นไม่สามารถวัดผลได้ตามวัตถุประสงค์ จากนั้นนำคะแนนเฉลี่ยเทียบกับเกณฑ์ที่ใช้ได้ คือ 0.5 (ล้วน สายยศ และอังคณา สายยศ, 2538, หน้า 248) ซึ่งได้ค่าเฉลี่ยคะแนนของแบบทดสอบผู้ใช้งานทั่วไปฯ เท่ากับ 0.83 และผู้ดูแลระบบ เท่ากับ 0.86

1.10 นำแบบสอบถามความพึงพอใจที่ผ่านการตรวจสอบแก้ไข จำนวน 22 ข้อ ที่ผู้วิจัยสร้างขึ้น ซึ่งเป็นฉบับสมบูรณ์ไปใช้กับกลุ่มตัวอย่าง

โดยกำหนดเกณฑ์ระดับความพึงพอใจออกเป็น

ตาราง 1 แสดงเกณฑ์ระดับความพึงพอใจ

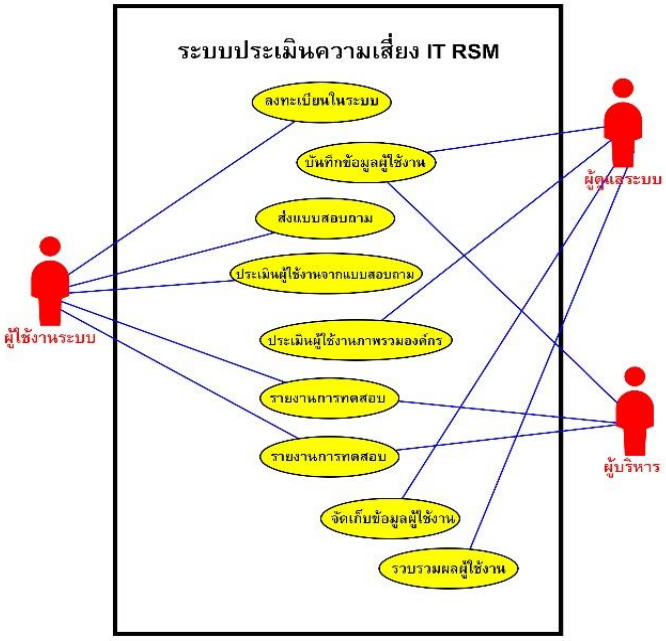
ค่าระดับ	แปรผลระดับความพึงพอใจ
4.51–5.00	มากที่สุด
3.51–4.50	มาก
2.51–3.50	ปานกลาง
1.51–2.50	น้อย
1–1.50	น้อยที่สุด

2. ทดสอบสร้างระบบประเมินระดับความเสี่ยง IT RSM

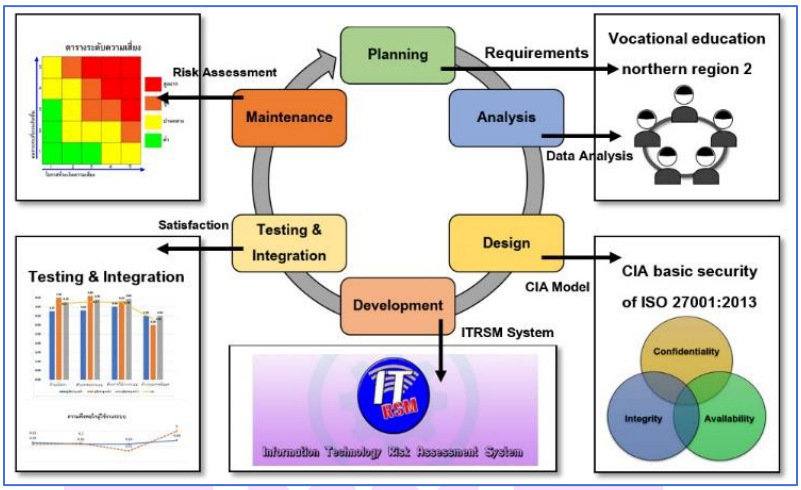
2.1 ศึกษาโปรแกรมการใช้งานที่มีการทำแบบทดสอบ ประมวลและจัดเก็บรวมรวมข้อมูลของผู้ใช้งาน อีกทั้งการรายงานผลการทดสอบ ปรากฏไม่พบโปรแกรมประยุกต์ที่ตรงกับความต้องการของผู้วิจัย จึงได้ทำการศึกษาเกี่ยวกับการสร้างและออกแบบระบบการใช้งานขึ้นเพื่อเป็นการอำนวยความสะดวกแก่ผู้ใช้งานและเพื่อให้มีการจัดเก็บรวมรวมข้อมูลการทำแบบทดสอบไว้

2.2 ได้ปรึกษากับทีมงานที่มีความรู้ในการสร้างระบบปฏิบัติการ ช่วยสร้างระบบขึ้นโดยใช้ชื่อว่า IT RSM และนำแบบทดสอบที่ได้ไปบรรจุไว้ในระบบและให้ระบบสามารถประมวลผลการประเมินและลำดับความเสี่ยงตามที่ผู้ใช้งานทำแบบทดสอบ และสามารถจัดเก็บรวบรวมข้อมูลผู้ใช้งานให้คงอยู่ในระบบ

2.3 นำระบบที่ได้ไปให้กลุ่มตัวอย่างทำการทดสอบเพื่อหาค่าความพึงพอใจการใช้งานของระบบ รวบรวมและสรุปผลการดำเนินงาน แบ่งผู้ใช้งานระบบได้เป็น 4 กลุ่มผู้ใช้งาน คือ ผู้ใช้งานทั่วไป เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ ผู้ดูแลระบบ และผู้บริหาร



ภาพ 5 แสดงการทำงานของ IT RSM (Use case Diagram)



ภาพ 6 แสดงวงจรการพัฒนาระบบสารสนเทศ (SDLC: System Develop Life Cycle)

2.4 ระบบประเมิน IT RSM ประกอบด้วย 4 ส่วน ซึ่งแสดงผลรายละเอียด ดังนี้

ส่วนที่ 1 หน้าเข้าสู่ระบบ เป็นหน้าสำหรับให้ผู้ใช้งานได้ลงทะเบียน เพื่อเก็บเป็นข้อมูลผู้ใช้งาน

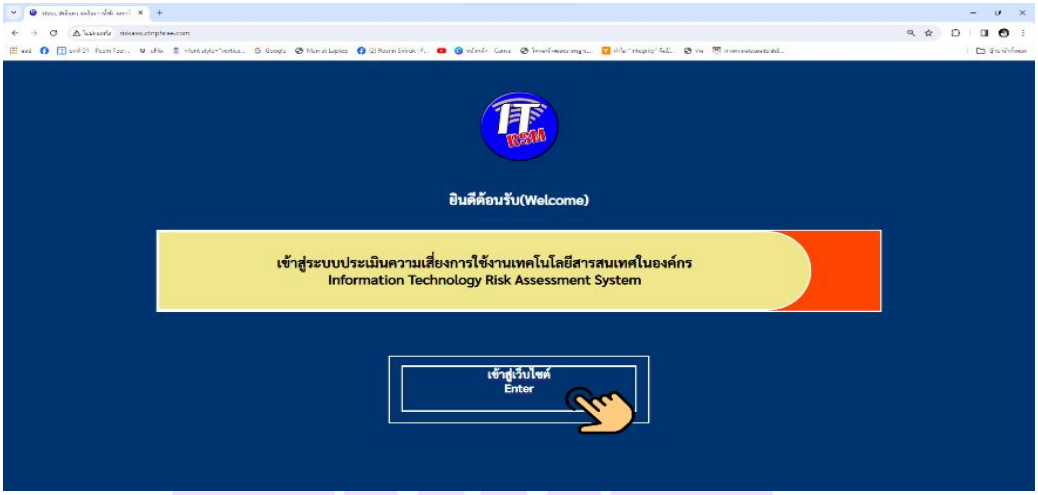
ส่วนที่ 2 หน้าทำแบบประเมิน แบ่งเป็นผู้และงานทั่วไปและผู้ดูแลระบบเข้าทำแบบทดสอบระบบตามตำแหน่งหน้าที่ของตนเอง

ส่วนที่ 3 หน้าแสดงผลการประเมิน หลังจากผู้ทำการทดสอบแล้วเสร็จจะแสดงผลโดยการแยกส่วนเฉพาะของผู้ทำแบบประเมิน

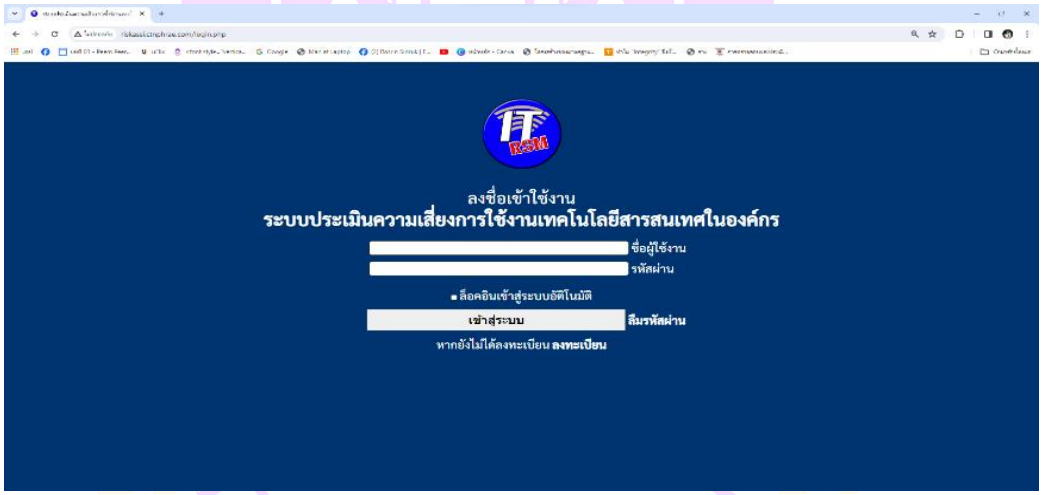
ส่วนที่ 4 หน้าแสดงคำแนะนำ จะแสดงผลโดยการบอกถึงข้อและแนวปฏิบัติของการใช้งานเทคโนโลยีสารสารเทศในองค์กรให้มีความมั่นคงปลอดภัย

ส่วนที่ 5 แสดงขั้นตอนการทำงานของระบบเบื้องต้นจากการทดลอง

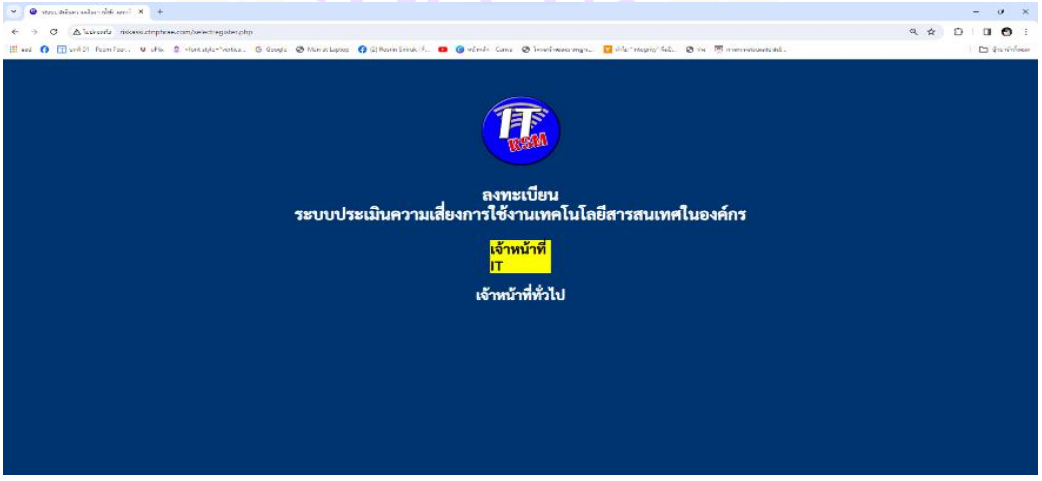
ลำดับการเข้าใช้งานแสดงหน้าจอ สำหรับกลุ่มตัวอย่าง



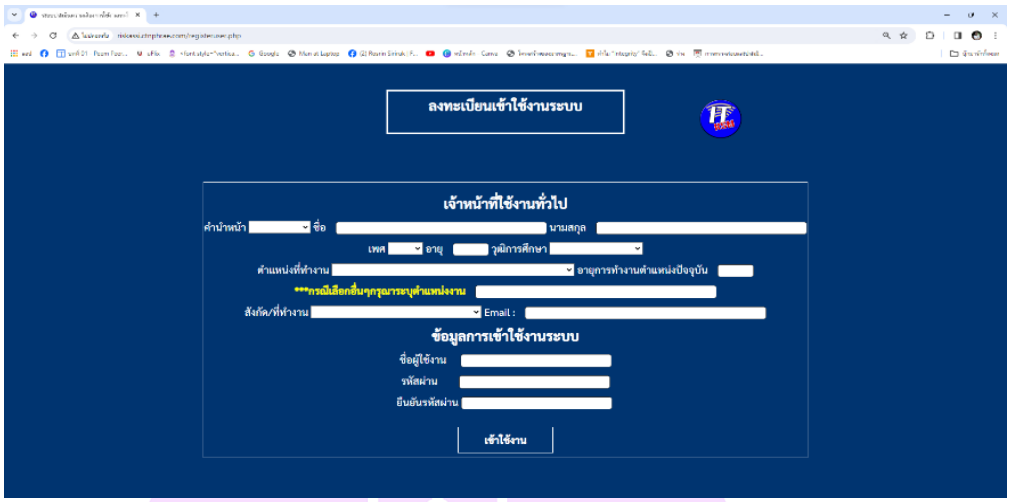
ภาพ 7 แสดงขั้นตอนที่ 1 หน้าแรกเข้าระบบ



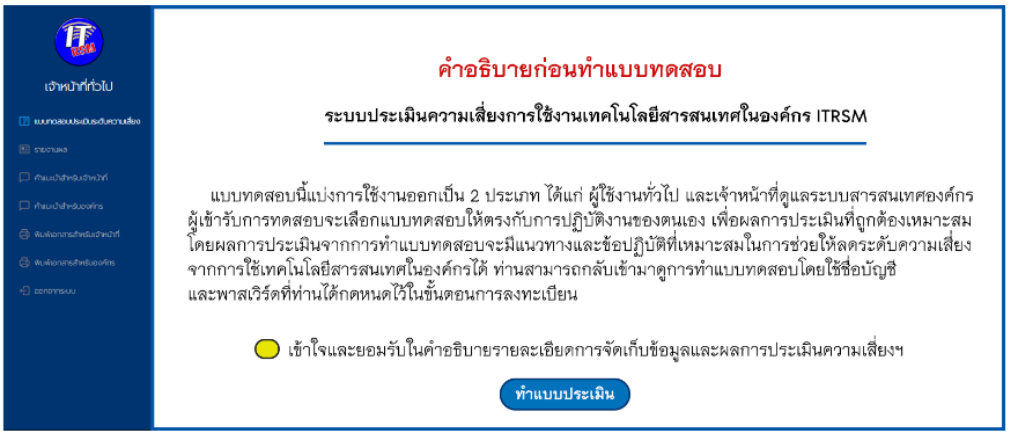
ภาพ 8 แสดงขั้นตอนที่ 2 หน้าที่ 2 ลงชื่อเข้าใช้งาน



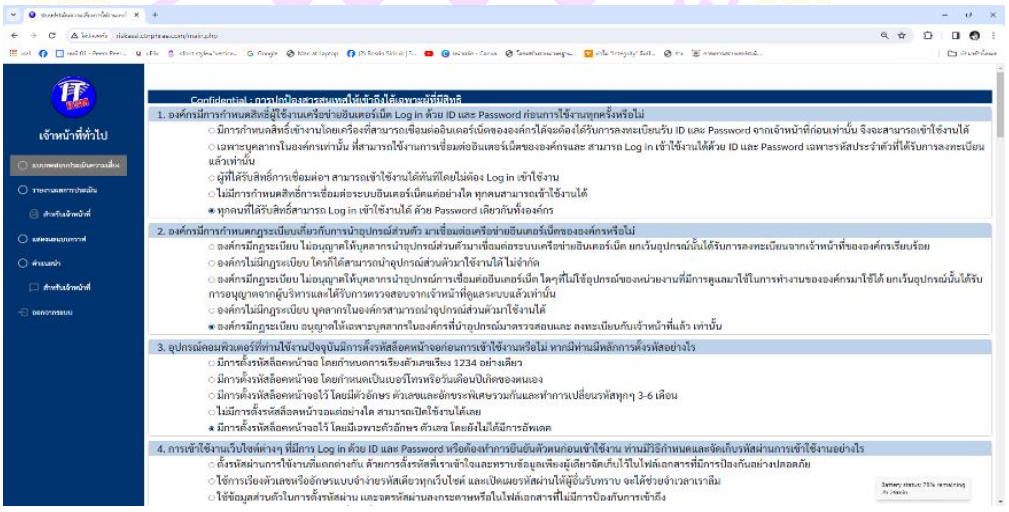
ภาพ 9 แสดงเลือกประเภทผู้เข้าใช้งานเพื่อการลงทะเบียน



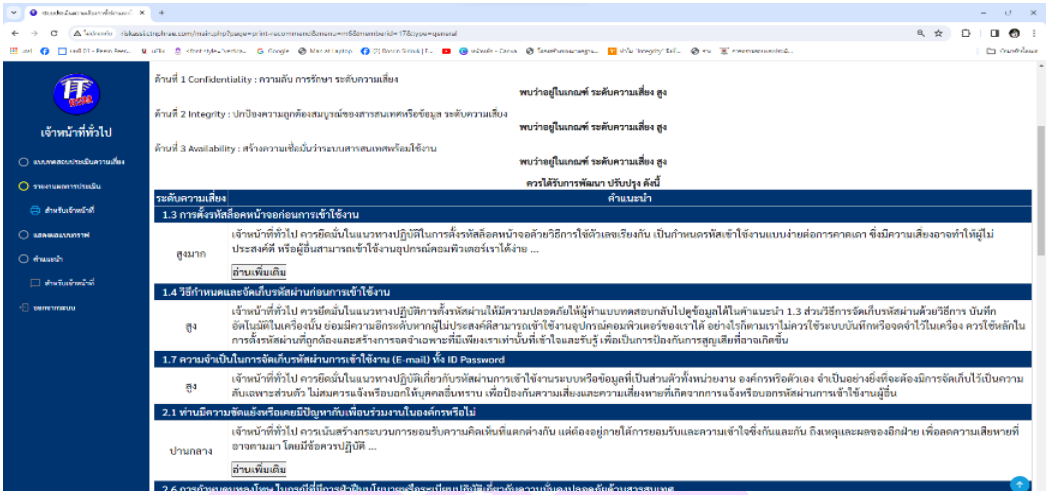
ภาพ 10 แสดงลงทะเบียนสร้างรหัสการเข้าใช้งาน



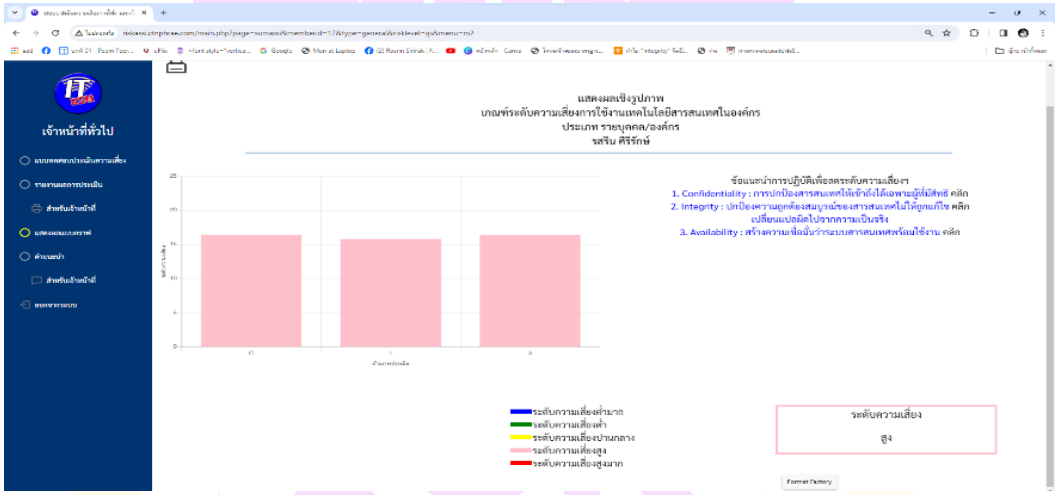
ภาพ 11 แสดงคำอธิบายก่อนการทำแบบทดสอบ



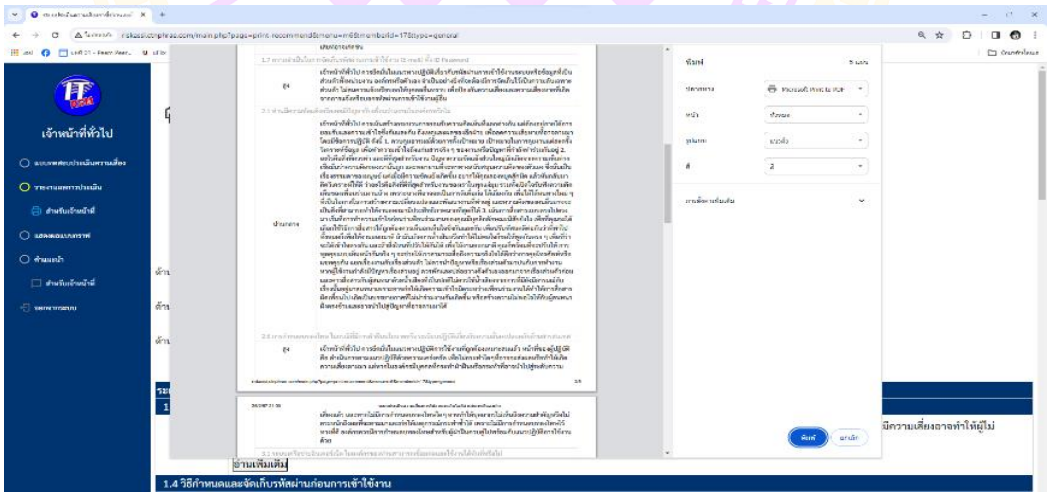
ภาพ 12 แสดงทำแบบประเมินความเสี่ยงตามประเภท



ภาพ 13 แสดงคำแนะนำการทำประเมินรายบุคคล

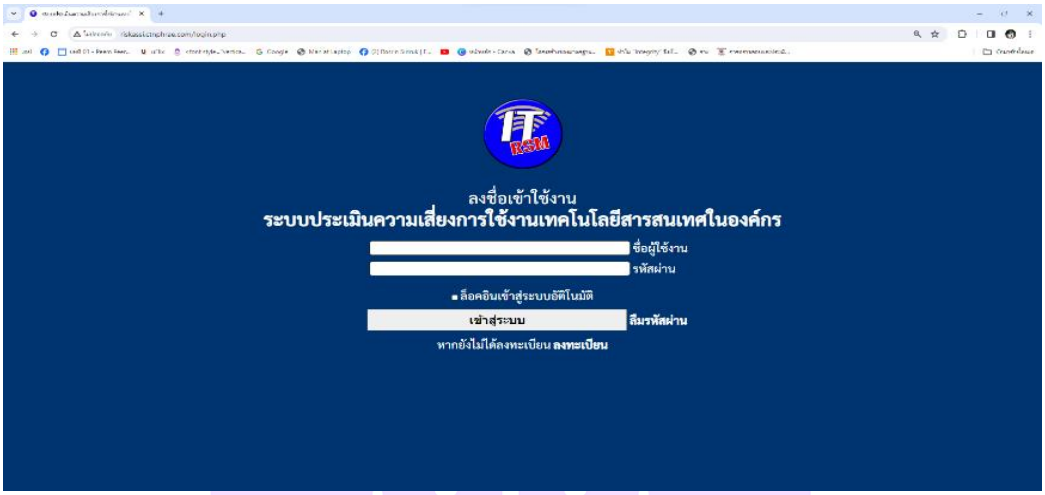


ภาพ 14 แสดงระบบรูปแบบ

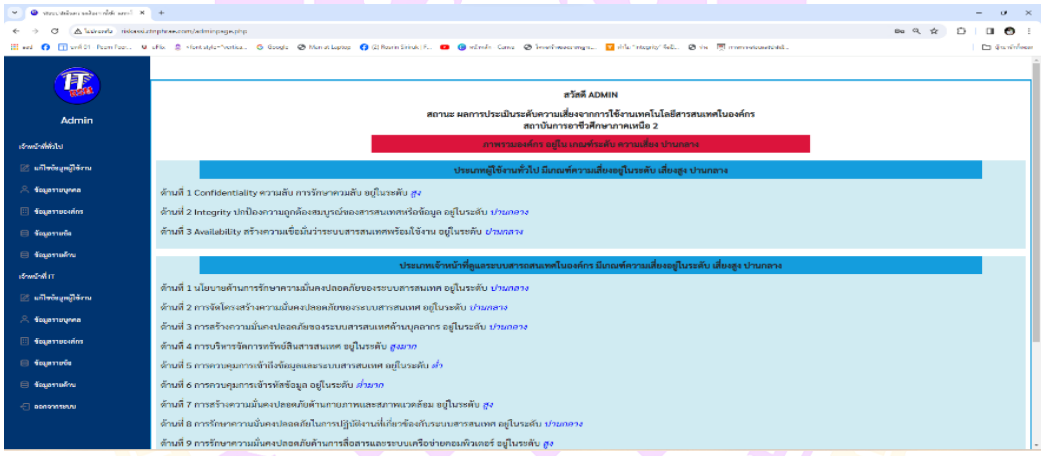


ภาพ 15 แสดงผลหน้าปริ้นคำแนะนำ

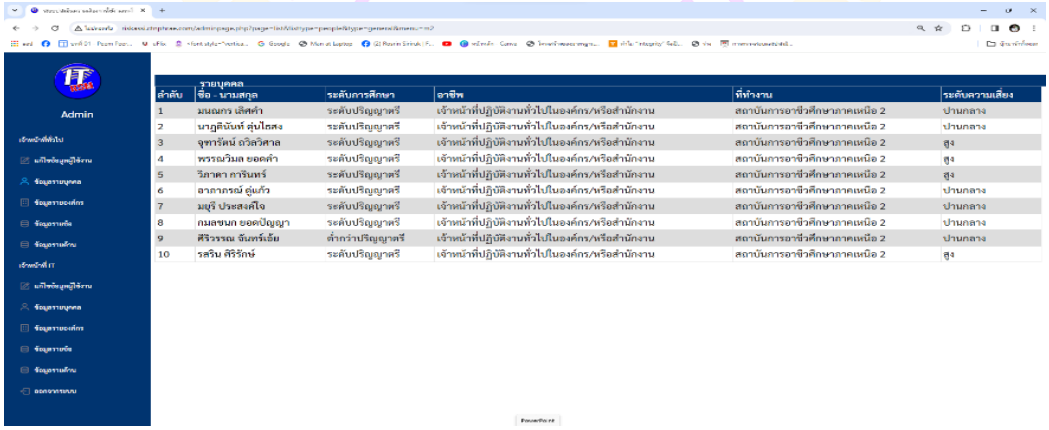
การแสดงผลหน้าจอ สำหรับ Adminและผู้บริหาร



ภาพ 16 แสดงการลงทะเบียนการเข้าใช้

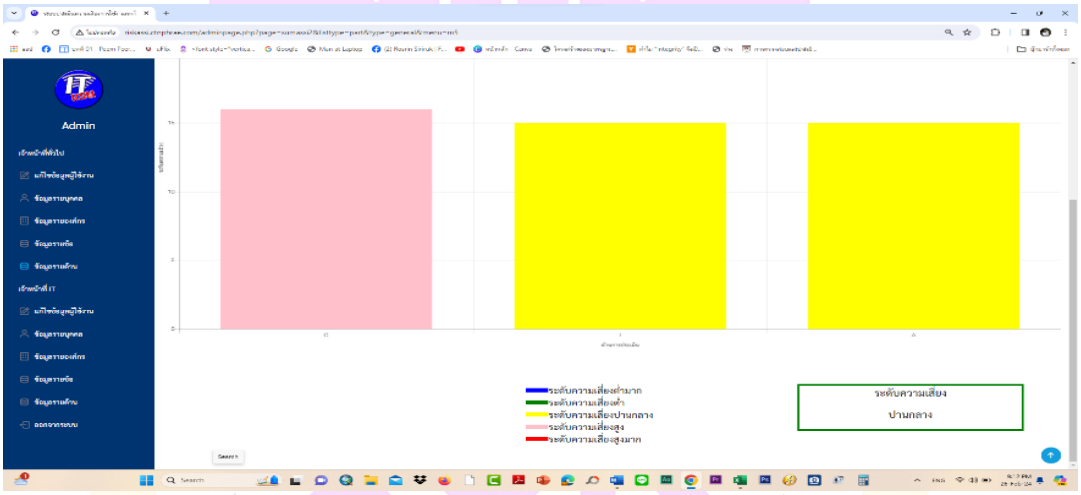


ภาพ 17 แสดงผลภาพรวมรายองค์กร



ภาพ 18 แสดงผลภาพรวมรายบุคคลในองค์กร

ภาพ 19 แสดงผลรายข้อ



ภาพ 20 แสดงผลรายด้าน

การกำหนดขั้นตอนในการดำเนินการวิจัย

1. ชี้แจงรายละเอียดข้อมูลการเข้าใช้งานและวิธีการทำแบบทดสอบ ให้กลุ่มตัวอย่างทั้ง 2 ประเภท ทราบ

2. ให้กลุ่มตัวอย่าง ทั้ง 2 ประเภท ทำแบบประเมินฯ ผ่านระบบ IT RSM

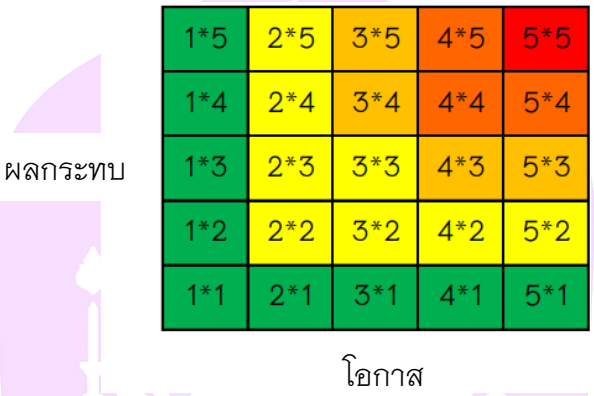
3. สอบถามความพึงพอใจของกลุ่มตัวอย่างทั้ง 2 กลุ่ม เพื่อประเมินผลการใช้งานระบบ IT RSM จากนั้นให้ทำแบบประเมินความพึงพอใจการใช้งานระบบฯ

4. วิเคราะห์และแปรผลข้อมูล

เนื่องด้วยระบบถูกทดสอบสร้างขึ้นอาจยังไม่สมบูรณ์และยังไม่รองรับข้อมูลทั้งหมดของกลุ่มผู้ใช้งาน ดังนั้น ผลการศึกษาความพึงพอใจการใช้งานระบบ ITRSM จึงยังไม่ถูกใช้กับกลุ่มผู้ใช้งานจะมีเพียงผลความพึงพอใจกับกลุ่มตัวอย่างก่อนเท่านั้น

ตาราง 3 แสดงระดับความรุนแรงของผลกระทบความเสี่ยงหากมีเหตุการณ์เกิดขึ้นโดย ระดับคะแนน 1 น้อยมาก ระดับคะแนน 2 น้อย ระดับคะแนน 3 ปานกลาง ระดับคะแนน 4 รุนแรงมาก และระดับคะแนน 5 รุนแรงมากที่สุด

ผลการประเมินความเสี่ยงสามารถแสดงในรูปแบบของ Risk Assessment Matrix ดังนี้



ภาพ 21 แผนผังประเมินความเสี่ยง (Risk Assessment Matrix)

ที่มา: จุฑามน สิทธิผลวนิชกุล, 2561

และการแปรผลระดับความเสี่ยงจะกำหนดได้ตามตาราง ดังนี้

ตาราง 2 แสดงการเทียบระดับความเสี่ยง

คำตอบ/ค่าระดับ	**แปรผลระดับความเสี่ยง**
1 = 1–5	เสี่ยงต่ำมาก
2 = 6–10	เสี่ยงต่ำ
3 = 11–15	ปานกลาง
4 = 16–20	เสี่ยงสูง
5 = 21–25	เสี่ยงสูงมาก

2. วิเคราะห์ความสอดคล้องของแบบทดสอบข้อมูลทั่วไปฯ ของกลุ่มตัวอย่างทั้ง 2 กลุ่ม โดยการหาค่าดัชนีความสอดคล้อง (Index of Consistency: IOC) จากสูตร(สมบูรณ์ สุริยะวงศ์ และคณะ, 2544, หน้า 84)

$$IOC = \frac{\sum R}{N}$$

IOC คือ ค่าดัชนีความสอดคล้อง

R คือ คะแนนของผู้เชี่ยวชาญ

$\sum R$ คือ ผลรวมคะแนนของผู้เชี่ยวชาญแต่ละคน

N คือ จำนวนผู้เชี่ยวชาญ

3. วิเคราะห์ความพึงพอใจของผู้ตอบแบบสอบถาม โดยใช้สถิติพื้นฐาน ได้แก่

3.1 ค่าร้อยละ (Percentage) จากสูตร (บุญชม ศรีสะอาด, หน้า 101)

$$P = \frac{F}{N} \times 100$$

P คือ ค่าคะแนนเฉลี่ย

F คือ ความถี่ของคะแนน

N คือ ขนาดของกลุ่มตัวอย่าง

3.2 ค่าเฉลี่ย (Mean) และค่าเบี่ยงเบนมาตรฐาน (Standard Deviation) จากสูตร (ล้วน สายยศ และอังคณา สายยศ, 2538, หน้า 73-76)

ค่าเฉลี่ย ($\overline{X}$) $= \frac{\sum X}{N}$

$\overline{X}$ คือ ค่าเฉลี่ย

$\sum X$ คือ ผลรวมของคะแนนทั้งหมดในกลุ่ม

N คือ จำนวนคนในกลุ่ม

ค่าเบี่ยงเบนมาตรฐาน (S.D.) $= \sqrt{\frac{\sum\left(\mathrm{X}-\bar{x}\right)^2}{N-1}}$

S.D. คือ ส่วนเบี่ยงเบนมาตรฐาน

x คือ คะแนนแต่ละตัว

$\overline{\mathrm{X}}$ คือ ค่าคะแนนเฉลี่ย

N คือ จำนวนคะแนนในกลุ่ม

$\sum$ คือ ผลรวม

การรายงานผลวิจัย

การวิจัยครั้งนี้นำเสนอผลการวิจัยในรูปแบบตารางและการพรรณนาวิเคราะห์

บทที่ 4

ผลการวิเคราะห์ข้อมูล

การศึกษาเรื่อง “การพัฒนาระบบประเมินความเสี่ยงการใช้เทคโนโลยีสารสนเทศให้ปลอดภัย ตามองค์ประกอบพื้นฐานความปลอดภัยสารสนเทศ CIAกรณีศึกษาสถาบันการอาชีวศึกษาภาคเหนือ 2” ผู้วิจัยได้แบ่งประเภทของประชากรกลุ่มตัวอย่าง ออกเป็น 2 ประเภท ได้แก่ 1. กลุ่มผู้ใช้งานทั่วไป จำนวน 10 คน และ 2. กลุ่มเจ้าหน้าที่ดูแลระบบประจำหน่วยงาน จำนวน 1 คน โดยสร้างระบบขึ้นมาเพื่อรองรับการบันทึกและจัดเก็บข้อมูลของประชากรกลุ่มตัวอย่าง ผ่านระบบประเมินความเสี่ยงที่มีชื่อว่า ITRSM ทำหน้าที่เป็นเครื่องมือประเมินระดับความเสี่ยง ประมวลผลข้อมูล และจัดเก็บข้อมูล โดยผู้วิจัยได้แบ่งการนำเสนอผลการวิจัยออกเป็นรายการต่าง ๆ ดังนี้

1. ผลการประเมินระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กรกรณีระดับองค์กร

2. ผลการประเมินระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กรของเจ้าหน้าที่ผู้ใช้งานระบบสารสนเทศในองค์กรสถาบันการอาชีวศึกษาภาคเหนือ 2 ซึ่งแบ่งเป็นกลุ่มเจ้าหน้าที่ผู้ใช้งานทั่วไปและกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร

3. ผลการประเมินระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กรของกลุ่มผู้ใช้งาน สถานศึกษาในสังกัด สถาบันการอาชีวศึกษาภาคเหนือ 2 จำนวน 9 แห่ง แบ่งเป็นกลุ่มเจ้าหน้าที่ทั่วไปและกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร

4. ผลการประเมินความพึงพอใจการใช้งานระบบประเมินความเสี่ยงเทคโนโลยีสารสนเทศในองค์กร (ITRSM) ขององค์กรในภาพรวม

5. ผลการประเมินความพึงพอใจการใช้งานระบบประเมินความเสี่ยงเทคโนโลยีสารสนเทศในองค์กร (ITRSM) ของกลุ่มตัวอย่าง

1. ผลการประเมินระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กร กรณีระดับองค์กรของกลุ่มตัวอย่าง สถาบันการอาชีวศึกษาภาคเหนือ 2

ตาราง 3 แสดงผลการประเมินระดับองค์กร รายด้าน ประเภทกลุ่มผู้ใช้งานทั่วไป

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	Confidentiality การรักษาความลับ	4	4	16	เสี่ยงสูง
2	Integrity ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไข	5	5	25	เสี่ยงสูงมาก
3	Availability สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน	5	5	25	เสี่ยงสูงมาก

จากตาราง 3 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร กรณีระดับองค์กร ของประเภทกลุ่มผู้ใช้งานทั่วไปขององค์กร พบว่า ด้านที่มีความเสี่ยงใน**ระดับที่สูงมาก** มี 2 ด้าน ได้แก่ ด้านที่ 2 I: Integrity การปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไข มีค่าระดับความเสี่ยงอยู่ที่ 25 และด้านที่ 3 A:Availability การสร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมา คือ ด้านที่มีความเสี่ยงใน**ระดับเสี่ยงสูง** ได้แก่ ด้านที่ 1 C: Confidentiality การรักษาความลับ มีค่าระดับความเสี่ยงอยู่ที่ 16

ตาราง 4 แสดงผลการประเมินระดับองค์กร รายด้าน ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก

ตางราง 4 (ต่อ) แสดงผลการประเมินระดับองค์กร รายด้าน ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
2	การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
3	การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร	5	5	25	เสี่ยงสูงมาก
4	การบริหารจัดการทรัพย์สินสารสนเทศ	5	5	25	เสี่ยงสูงมาก
5	การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ	4	5	20	เสี่ยงสูง
6	การควบคุมการเข้ารหัสข้อมูล	5	5	25	เสี่ยงสูงมาก
7	การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม	4	5	20	เสี่ยงสูง
8	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ	5	4	20	เสี่ยงสูง
9	การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์	5	5	25	เสี่ยงสูงมาก
10	การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ	5	4	20	เสี่ยงสูง
11	การควบคุมดูแลผู้ให้บริการภายนอก	5	5	25	เสี่ยงสูงมาก

ตาราง 4 (ต่อ) แสดงผลการประเมินระดับองค์กร รายด้าน ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
12	การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
13	การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	4	3	12	ปานกลาง
14	การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด	5	5	25	เสี่ยงสูงมาก
	รวม			**22**	**เสี่ยงสูงมาก**

จากตาราง 4 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร กรณีระดับองค์กร ของประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่ามีความเสี่ยงใน**ระดับที่สูงมาก** และหากจะพิจารณาเป็นรายด้าน พบว่า ด้านที่มีความเสี่ยงใน**ระดับที่สูงมาก มี 9 ด้าน** ได้แก่ ด้านที่ 1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ มีค่าระดับความเสี่ยงอยู่ที่ 25 ด้านที่ 2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ มีค่าระดับความเสี่ยงอยู่ที่ 25 ด้านที่ 3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร มีค่าระดับความเสี่ยงอยู่ที่ 25 ด้านที่ 4 การบริหารจัดการทรัพย์สินสารสนเทศ มีค่าระดับความเสี่ยงอยู่ที่ 25 ด้านที่ 6 การควบคุมการเข้ารหัสข้อมูล มีค่าระดับความเสี่ยงอยู่ที่ 25 ด้านที่ 9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ มีค่าระดับความเสี่ยงอยู่ที่ 25 ด้านที่ 11 การควบคุมดูแลผู้ให้บริการภายนอก มีค่าระดับความเสี่ยงอยู่ที่ 25 ด้านที่ 12 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ มีค่าระดับความเสี่ยงอยู่ที่ 25 และด้านที่ 14 การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมา คือ ด้านที่มี**ระดับความเสี่ยงสูง มี 4 ด้าน** ได้แก่ ด้านที่ 5 การควบคุมการเข้าถึง

ข้อมูลและระบบสารสนเทศ มีค่าระดับความเสี่ยงอยู่ที่ 20 ด้านที่ 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม มีค่าระดับความเสี่ยงอยู่ที่ 20 ด้านที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ มีค่าระดับความเสี่ยงอยู่ที่ 20 และด้านที่ 10 การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ มีค่าระดับความเสี่ยงอยู่ที่ 20 สำหรับด้านที่มี**ระดับความเสี่ยงปานกลาง มี 1 ด้าน** ได้แก่ ด้านที่ 13 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ มีค่าระดับความเสี่ยงอยู่ที่ 12

2. ผลการประเมินระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กรของเจ้าหน้าที่ผู้ใช้งานระบบในองค์กรสถาบันการอาชีวศึกษาภาคเหนือ 2 ซึ่งแบ่งเป็นกลุ่มเจ้าหน้าที่ผู้ใช้งานทั่วไปและกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร

กลุ่มผู้ใช้งานทั่วไป

ส่วนที่ 1 ผลการวิเคราะห์ข้อมูลทั่วไปของประชากรกลุ่มตัวอย่าง

ส่วนที่ 2 ผลการวิเคราะห์พฤติกรรมการใช้งานเทคโนโลยีสารสนเทศในองค์กรตามหลักองค์ประกอบพื้นฐาน CIA (Confidentiality Integrity และ Availability)

ส่วนที่ 1 ผลการวิเคราะห์ข้อมูลทั่วไปของประชากรกลุ่มตัวอย่าง

ตาราง 5 แสดงจำนวนและร้อยละจำแนกตามลักษณะทางประชากรของกลุ่มตัวอย่าง

ลักษณะทางประชากร	จำนวน (คน)	ร้อยละ
1. ตำแหน่งงานปัจจุบัน		
เจ้าหน้าที่ปฏิบัติงานทั่วไปในองค์กร/สำนักงาน	10	100
2. อายุ		
-ระหว่าง 18-29 ปี	3	30
-ระหว่าง 30-44 ปี	6	60
-ระหว่าง 45-59 ปี	1	10

ตาราง 5 (ต่อ) แสดงจำนวนและร้อยละจำแนกตามลักษณะทางประชากรของกลุ่มตัวอย่าง

ลักษณะทางประชากร	จำนวน (คน)	ร้อยละ
3. เพศ		
หญิง	10	100
4. อายุการทำงานถึงปัจจุบัน		
-1-4 ปี	1	10
-5-10 ปี	7	70
-11-15 ปี	1	10
-16-20 ปี	1	10
5. อุปกรณ์คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการเชื่อมต่ออินเตอร์เน็ตในการทำงานประจำ		
-ที่ทำงาน	3	30
-ของส่วนตัว	1	10
-ทั้งของที่ทำงานและส่วนตัว	6	60

จากตาราง 5 แสดงลักษณะประชากรที่ศึกษาทั้งสิ้น 10 คน จำแนกลักษณะประชากรได้ดังนี้

ตำแหน่งงาน ณ ปัจจุบัน เป็นเจ้าหน้าที่ปฏิบัติงานทั่วไปในองค์กร/สำนักงาน จำนวน 10 คน คิดเป็นร้อยละ 100

อายุ กลุ่มตัวอย่างมีอายุอยู่ในช่วงระหว่าง 30-40 ปี มากที่สุด จำนวน 6 คน คิดเป็นร้อยละ 60 รองลงมาคือช่วงอายุ 18-29 ปี จำนวน 3 คน คิดเป็นร้อยละ 30 และช่วงอายุ 45-59 ปี จำนวน 1 คน คิดเป็นร้อยละ 10 ตามลำดับ

เพศ กลุ่มตัวอย่างทั้งหมดเป็นเพศหญิง จำนวน 10 คน คิดเป็นร้อยละ 100

อายุการทำงานถึงปัจจุบัน กลุ่มตัวอย่างมีอายุการทำงานอยู่ระหว่าง 5-10 ปี จำนวน 7 คน คิดเป็นร้อยละ 70 รองลงมามีอายุการทำงานเท่ากัน คือ 1 ปี คิดเป็นร้อยละ 30

อุปกรณ์คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการเชื่อมต่ออินเตอร์เน็ตในการทำงานประจำ ประชากรกลุ่มตัวอย่างมีอุปกรณ์คอมพิวเตอร์ที่ใช้ทำงานเป็นประจำทุกวัน โดยใช้ทั้งของส่วนตัวและของที่ทำงาน จำนวน 6 คน คิดเป็นร้อยละ 60 รองลงมา คือ ใช้ของที่ทำงาน จำนวน 3 คน คิดเป็นร้อยละ 30 และใช้ของส่วนตัว จำนวน 1 คน คิดเป็นร้อยละ 10 ตามลำดับ

ส่วนที่ 2 ผลการวิเคราะห์พฤติกรรมการใช้งานเทคโนโลยีสารสนเทศในองค์กรตามหลักองค์ประกอบพื้นฐาน CIA แบ่งออกเป็น 3 ด้าน ซึ่งประกอบไปด้วย ด้านที่ 1 Confidentiality : การรักษาความลับ ด้านที่ 2 Integrity : ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความเป็นจริง ด้านที่ 3 Availability : สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งานการตอบสนองความต้องการของผู้ใช้งานที่มี

ตาราง 6 แสดงด้านที่ 1 Confidentiality: การรักษาความลับ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีการกำหนดสิทธิ์ผู้ใช้งานเครือข่ายอินเตอร์เน็ต Log in ด้วย ID และ Password ก่อนการใช้งานทุกครั้งหรือไม่	5	4	20	เสี่ยงสูง
2	องค์กรมีการกำหนดกฎระเบียบเกี่ยวกับการนำอุปกรณ์ส่วนตัวมาเชื่อมต่อเครือข่ายอินเตอร์เน็ตขององค์กรหรือไม่	5	4	20	เสี่ยงสูง
3	อุปกรณ์คอมพิวเตอร์ที่ท่านใช้งานปัจจุบันมีการตั้งรหัสล็อคหน้าจอก่อนการเข้าใช้งานหรือไม่ หากมีท่านมีหลักการตั้งรหัสอย่างไร	4	5	20	เสี่ยงสูง

ตาราง 6 (ต่อ) แสดงด้านที่ 1 Confidentiality: การรักษาความลับ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
4	การเข้าใช้งานเว็บไซต์ต่าง ๆ ที่มีการ Log in ด้วย ID และ Password หรือต้องทำการยืนยันตัวตนก่อนเข้าใช้งาน ท่านมีวิธีกำหนดและจัดเก็บรหัสผ่าน1 การเข้าใช้งานอย่างไร	4	3	12	ปานกลาง
5	องค์กรท่านมีการกำหนดนโยบายเกี่ยวกับสิทธิในการเข้าถึงข้อมูลเทคโนโลยีสารสนเทศในองค์กรหรือไม่ ท่านปฏิบัติอย่างไรกับนโยบายดังกล่าว	5	5	25	เสี่ยงสูงมาก
6	องค์กรของท่านมีการจัดทำแผนพัฒนาระบบสารสนเทศในองค์กรหรือไม่ ใครเป็นผู้ร่วมดำเนินการตามแผนดังกล่าว	5	4	20	เสี่ยงสูง
7	ท่านคิดว่าการจัดเก็บรหัสผ่านการเข้าใช้งาน (E-mail) ทั้ง ID Password มีความจำเป็นหรือไม่ที่จะจัดเก็บเป็นความลับ และใครบ้างที่สามารถทราบรหัสผ่านการรเข้าใช้งานของท่านได้	3	3	9	ต่ำ

จากตาราง 6 แสดงผลการวิเคราะห์พฤติกรรมการใช้งานเทคโนโลยีสารสนเทศของเจ้าหน้าที่ทั่วไป ด้านที่ 1 Confidentiality: การรักษาความลับ ของกลุ่มเจ้าหน้าที่ทั่วไปในสถาบันการอาชีวศึกษาภาคเหนือ 2 จำนวน 10 คน พบว่า ข้อที่มีความเสี่ยงอยู่ใน **ระดับเสี่ยงสูงมาก** ได้แก่ ข้อที่ 5 องค์กรท่านมีการกำหนดนโยบายเกี่ยวกับสิทธิในการเข้าถึงข้อมูลเทคโนโลยีสารสนเทศในองค์กรหรือไม่ ท่านปฏิบัติอย่างไรกับนโยบายดังกล่าว มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมาอยู่ใน **ระดับความเสี่ยงสูง** ได้แก่ ข้อ 1 องค์กรมีการกำหนดสิทธิ์ผู้ใช้งาน

เครือข่ายอินเตอร์เน็ต Log in ด้วย ID และ Password ก่อนการใช้งานทุกครั้งหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 2 องค์กรมีการกำหนดกฎระเบียบเกี่ยวกับการนำอุปกรณ์ส่วนตัวมาเชื่อมต่อเครือข่ายอินเตอร์เน็ตขององค์กรหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 3 อุปกรณ์คอมพิวเตอร์ที่ท่านใช้งานปัจจุบันมีการตั้งรหัสล็อคหน้าจอก่อนการเข้าใช้งานหรือไม่ หากมีท่านมีหลักการ ตั้งรหัสอย่างไร มีค่าระดับความเสี่ยงอยู่ที่ 20 และข้อ 6 องค์กรของท่านมีการจัดทำแผนพัฒนาระบบสารสนเทศในองค์กรหรือไม่ ใครเป็นผู้ร่วมดำเนินการตามแผนดังกล่าว มีค่าระดับความเสี่ยงอยู่ที่ 20 สำหรับความเสี่ยงใน **ระดับปานกลาง** ได้แก่ ข้อ 4 การเข้าใช้งานเว็บไซต์ต่าง ๆ ที่มีการ Log in ด้วย ID และ Password หรือต้องทำการยืนยันตัวตนก่อนเข้าใช้งาน ท่านมีวิธีกำหนดและจัดเก็บรหัสผ่านการเข้าใช้งานอย่างไร มีค่าระดับความเสี่ยงอยู่ที่ 12 และความเสี่ยงใน **ระดับต่ำ** ได้แก่ ข้อ 7 ท่านคิดว่าการจัดเก็บรหัสผ่านการเข้าใช้งาน E-mail ทั้ง ID Password มีความจำเป็นหรือไม่ที่จะจัดเก็บเป็นความลับ และใครบ้างที่สามารถทราบรหัสผ่านการรเข้าใช้งานของท่านได้ มีค่าระดับความเสี่ยงอยู่ที่ 9

ตาราง 7 แสดงด้านที่ 2 Integrity : ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	ท่านมีความขัดแย้งหรือเคยมีปัญหากับเพื่อนร่วมงานในองค์กรหรือไม่	4	3	12	ปานกลาง
2	คุณมีวิธีการสำรองข้อมูลในงานที่รับผิดชอบอย่างไร	4	5	20	เสี่ยงสูง
3	ใครบ้างที่สามารถเข้าใช้งานเครื่องคอมพิวเตอร์ที่ใช้งานประจำของท่านได้	5	5	25	เสี่ยงสูงมาก
4	ท่านมีการอัพเดตการใช้งานโปรแกรม Anti Virus เครื่องที่ใช้งานประจำหรือไม่ ใครเป็นผู้ดำเนินการให้	5	4	20	เสี่ยงสูง
5	ทุกครั้งที่เกิดปัญหาจากการใช้งานเทคโนโลยีสารสนเทศในองค์กรท่านมีวิธีจัดการอย่างไร	5	5	25	เสี่ยงสูงมาก

ตาราง 7 (ต่อ) แสดงด้านที่ 2 Integrity : ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
6	องค์กรมีการกำหนดบทลงโทษในกรณีที่มีการฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศและได้มีการปฏิบัติตามกฎดังกล่าวหรือไม่	5	5	25	เสี่ยงสูงมาก

จากตาราง 7 แสดงผลการวิเคราะห์พฤติกรรมการใช้งานเทคโนโลยีสารสนเทศของเจ้าหน้าที่ทั่วไป ด้านที่ 2 Integrity: ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความเป็นจริง ของกลุ่มเจ้าหน้าที่ทั่วไปในสถาบันการอาชีวศึกษาภาคเหนือ 2 จำนวน 10 คน พบว่า ที่มีความเสี่ยงอยู่ใน **ระดับเสี่ยงสูงมาก** ได้แก่ ข้อ 3 ใครบ้างที่สามารถเข้าใช้งานเครื่องคอมพิวเตอร์ที่ใช้งานประจำของท่านได้ มีค่าระดับความเสี่ยงอยู่ที่ 25 ข้อ 5 ทุกครั้งที่เกิดปัญหาจากการใช้งานเทคโนโลยีสารสนเทศในองค์กรท่านมีวิธีจัดการอย่างไร มีค่าระดับความเสี่ยงอยู่ที่ 25 และข้อ 6 องค์กรมีการกำหนดบทลงโทษในกรณีที่มีการฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัย ด้านสารสนเทศและได้มีการปฏิบัติตามกฎดังกล่าวหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมามีความเสี่ยงอยู่ใน **ระดับเสี่ยงสูง** ได้แก่ ข้อ 2 คุณมีวิธีการสำรองข้อมูลในงานที่รับผิดชอบอย่างไร มีค่าระดับความเสี่ยงอยู่ที่ 20 และข้อ 4 ท่านมีการอัพเดตการใช้งานโปรแกรม Anti Virus เครื่องที่ใช้งานประจำหรือไม่ใครเป็นผู้ดำเนินการให้ มีค่าระดับความเสี่ยงอยู่ที่ 20 สำหรับความเสี่ยงใน **ระดับปานกลาง** ได้แก่ ข้อ 1 ท่านมีความขัดแย้งหรือเคยมีปัญหากับเพื่อนร่วมงานในองค์กรหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 12

ตาราง 8 แสดงด้านที่ 3 Availability: ความเชื่อมั่นระบบสารสนเทศพร้อมใช้งาน

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	ระบบเครือข่ายอินเตอร์เน็ตในองค์กรของท่านสามารถเชื่อมต่อและใช้งานได้ทันทีหรือไม่	5	5	25	เสี่ยงสูงมาก
2	ท่านได้มีการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ที่ใช้งานเป็นประจำสม่ำเสมอหรือไม่	5	4	20	เสี่ยงสูง
3	ท่านเคยได้รับการอบรมให้ความรู้เกี่ยวกับการใช้ระบบสารสนเทศที่ปลอดภัยภายในองค์กรหรือไม่	5	5	25	เสี่ยงสูงมาก
4	ทราบหรือไม่ว่า โปรแกรมการใช้งานต่าง ๆ บนอุปกรณ์คอมพิวเตอร์ในสำนักงานของท่าน มีที่มาจากแหล่งใดและเป็นโปรแกรมที่ถูกต้องตามลิขสิทธิ์หรือไม่	5	5	25	เสี่ยงสูงมาก
5	คุณมีวิธีปฏิบัติอย่างไร เมื่อมีเหตุให้ต้องลุกออกจากการใช้งานหน้าคอมพิวเตอร์ที่กำลังใช้งานอยู่	4	5	20	เสี่ยงสูง
6	คุณมีหลักหรือแนวทางปฏิบัติในการตั้งไอดีและพาสเวิร์ดเข้าใช้งานเว็บไซต์ต่าง ๆอย่างไร	5	5	25	เสี่ยงสูงมาก
7	ความถี่ในการเข้าเปลี่ยนรหัสการใช้งานทั้งเว็บไซต์และอุปกรณ์สารสนเทศต่าง ๆ ของคุณคือ	4	5	20	เสี่ยงสูง

ตาราง 8 (ต่อ) แสดงด้านที่ 3 Availability: สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
8	ท่านกำหนดรหัสการเข้าใช้งานเว็บไซต์และอุปกรณ์ต่าง ๆ ด้วยรหัสผ่านเดียวกัน หรือไม่	4	4	16	สูง
9	ท่านรู้จักระบบปฏิบัติการที่ใช้ในการจัดเก็บข้อมูลทางระบบออนไลน์อย่างเช่น Cloud หรือ Google Dive หรือไม่	3	4	12	ปานกลาง
10	เครื่องคอมพิวเตอร์ที่ท่านใช้งานเคยติดไวรัส หรือมัลแวร์หรือไม่	4	4	16	เสี่ยงสูง
11	ท่านอนุญาตให้เพื่อนร่วมงานนำแฟลซไดร์ฟมาบันทึกไฟล์งานหรือข้อมูลต่าง ๆ ยังเครื่องที่ท่านใช้งานหรือไม่	5	5	25	เสี่ยงสูงมาก
12	ท่านเคยได้รับอีเมล์หรือข้อความที่ไม่ทราบแหล่งที่มาหรือไม่และท่านปฏิบัติอย่างไรเมื่อได้รับอีเมลนั้น	5	5	25	เสี่ยงสูงมาก
13	ท่านทราบหรือไม่ว่าไวรัสหรือมัลแวร์สามารถทำลายข้อมูลระบบและข้อมูลขององค์กรได้จากเครื่องที่ท่านใช้งานได้	4	5	20	เสี่ยงสูง
14	ท่านต้องการได้รับการอบรมความปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศเพิ่มเติมหรือไม่และควรมีช่วงเวลารับการอบรมเท่าไหร่จึงจะเหมาะสมในความคิดของท่าน	4	4	16	สูง

จากตาราง 8 แสดงผลการวิเคราะห์พฤติกรรมการใช้งานเทคโนโลยีสารสนเทศของเจ้าหน้าที่ทั่วไป ด้านที่ 3 Availability: สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งานการตอบสนองความต้องการของผู้ใช้งานที่มี ของกลุ่มเจ้าหน้าที่ทั่วไปในสถานบันการอาชีวศึกษาภาคเหนือ 2 จำนวน 10 คน พบว่า ข้อที่มีความเสี่ยงอยู่ใน **ระดับเสี่ยงสูงมาก** ได้แก่ ข้อ 1 ระบบเครือข่ายอินเตอร์เน็ตในองค์กรของท่านสามารถเชื่อมต่อและใช้งานได้ทันทีหรือไม่มีค่าระดับความเสี่ยงอยู่ที่ 25 ข้อ 3 ท่านเคยได้รับการอบรมให้ความรู้เกี่ยวการใช้ระบบสารสนเทศที่ปลอดภัยภายในองค์กรหรือไม่มีค่าระดับความเสี่ยงอยู่ที่ 25 ข้อ 4 ทราบหรือไม่ว่าโปรแกรมการใช้งานต่าง ๆ บนอุปกรณ์คอมพิวเตอร์ในสำนักงานของท่านมีที่มาจากแหล่งใดและเป็นโปรแกรมที่ถูกต้องตามลิขสิทธิ์หรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 ข้อ 6 คุณมีหลักหรือแนวทางปฏิบัติในการในการตั้งไอดีและพาสเวิร์ดเข้าใช้งานเว็บไซต์ต่าง ๆ อย่างไรมีค่าระดับความเสี่ยงอยู่ที่ 25 ข้อ 11 ท่านอนุญาตให้เพื่อนร่วมงานนำแฟลชไดร์ฟมาบันทึกไฟล์งานหรือข้อมูลต่าง ๆ ยังเครื่องที่ท่านใช้งานหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 และข้อ 12 ท่านเคยได้รับอีเมล์หรือข้อความที่ไม่ทราบแหล่งที่มาหรือไม่ และท่านปฏิบัติอย่างไรเมื่อได้รับอีเมลนั้น มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมามีความเสี่ยงอยู่ใน **ระดับเสี่ยงสูง** ได้แก่ ข้อ 2 ท่านได้มีการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ที่ใช้งานเป็นประจำสม่ำเสมอหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 5 คุณมีวิธีปฏิบัติอย่างไร เมื่อมีเหตุให้ต้องลุกออกจากการใช้งานหน้าคอมพิวเตอร์ที่กำลังใช้งานอยู่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 7 ความถี่ในการเข้าเปลี่ยนรหัสการใช้งานทั้งเว็บไซต์และอุปกรณ์สารสนเทศต่าง ๆ ของคุณคือ มีค่าระดับความเสี่ยงอยู่ที่ 20ข้อ 13 ท่านทราบหรือไม่ว่าไวรัสหรือมัลแวร์ สามารถทำลายข้อมูลระบบและข้อมูลขององค์กรได้จากเครื่องที่ท่านใช้งานได้ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 8 ท่านกำหนดรหัสการเข้าใช้งานเว็บไซต์และอุปกรณ์ต่าง ๆ ด้วยรหัสผ่านเดียวกันหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 16ข้อ 10 เครื่องคอมพิวเตอร์ที่ท่านใช้งานเคยติดไวรัส หรือมัลแวร์ หรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 16 และข้อ 14 ท่านต้องการได้รับการอบรมความปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศเพิ่มเติมหรือไม่ และควรมีช่วงเวลารับการอบรมเท่าไหร่จึงจะเหมาะสมในความคิดของท่านมีค่าระดับความเสี่ยงอยู่ที่ 16 สำหรับความเสี่ยงอยู่ใน **ระดับปานกลาง** ได้แก่ ข้อ 9 ท่านรู้จักระบบปฏิบัติการที่ใช้ในการจัดเก็บข้อมูลทางระบบออนไลน์ อย่างเช่น Cloud หรือ Google Dive หรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 12

กลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร

ส่วนที่ 1 ผลการวิเคราะห์ข้อมูลทั่วไปของประชากรกลุ่มตัวอย่าง

ส่วนที่ 2 ผลการวิเคราะห์พฤติกรรมการใช้งานเทคโนโลยีสารสนเทศในองค์กรอ้างอิงตามหลักมาตรฐานความปลอดภัยเทคโนโลยีสารสนเทศ ISO 270001

ส่วนที่ 1 ผลการวิเคราะห์ข้อมูลทั่วไปของประชากรกลุ่มตัวอย่าง

ตาราง 9 แสดงจำนวนและร้อยละจำแนกตามลักษณะทางประชากรของกลุ่มตัวอย่าง

ลักษณะทางประชากร	จำนวน (คน)	ร้อยละ
1. ตำแหน่งงานปัจจุบัน		
เจ้าหน้าที่ดูแลเกี่ยวกับระบบสารสนเทศองค์กร	1	100
2. อายุ		
ระหว่าง 30–44 ปี	1	100
3. เพศ		
ชาย	1	100
4. อายุการทำงานถึงปัจจุบัน		
5–10 ปี	1	100
5. ประสบการณ์ในการทำงานด้าน		
เทคโนโลยีสารสนเทศ	1	100
5–10 ปี		

จากตาราง 9 แสดงลักษณะประชากรที่ศึกษาเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร สถาบันการอาชีวศึกษาภาคเหนือ 2 จำนวน 1 คน จำแนกลักษณะประชากรได้ ดังนี้

ตำแหน่งงาน ณ ปัจจุบัน เจ้าหน้าที่ดูแลเกี่ยวกับระบบสารสนเทศองค์กร จำนวน 1 คน คิดเป็นร้อยละ 100

อายุ ระหว่าง 30–44 ปี

เพศ ชาย

มีประสบการณ์ในการทำงานด้านเทคโนโลยีสารสนเทศ 5–10 ปี

ส่วนที่ 2 ผลการวิเคราะห์พฤติกรรมการใช้งานเทคโนโลยีสารสนเทศในองค์กร ผู้ดูแลระบบสารสนเทศในองค์กร หรือผู้มีส่วนเกี่ยวข้องในการบริหารจัดการกับระบบสารสนเทศในองค์กร อ้างอิงจากโครงสร้างมาตรฐาน ISO 27001:2013 แบ่งเนื้อหาออกเป็น 14 ด้าน

ตาราง 10 แสดงด้านที่ 1 นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีการจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษรและได้รับอนุมัติจากผู้บริหาร รวมทั้งมีการสื่อสารให้บุคลากรในองค์กรรับทราบหรือไม่	5	5	25	เสี่ยงสูงมาก
2	นโยบายความมั่นคงปลอดภัยสารสนเทศมีเนื้อหาที่เหมาะสม ครบถ้วนเพียงพอ และได้รับการทบทวนตามรอบระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงหรือไม่	5	5	25	เสี่ยงสูงมาก

จากตางราง 10 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่า ด้านที่ 1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อที่มี **ระดับความเสี่ยงสูงมาก** ได้แก่ ข้อ 1 องค์กรมีการจัดทำนโยบาย ความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษรและได้รับอนุมัติจากผู้บริหาร รวมทั้งมีการสื่อสารให้บุคลากรในองค์กรรับทราบหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 และข้อ 2 นโยบายความมั่นคงปลอดภัยสารสนเทศมีเนื้อหาที่เหมาะสม ครบถ้วนเพียงพอ และได้รับการทบทวนตามรอบระยะเวลาที่กำหนดหรือเมื่อมีการเปลี่ยนแปลงหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25

ตาราง 11 แสดงด้านที่ 2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีการกำหนดขอบเขตและมอบหมายหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศให้แก่พนักงานภายในองค์กร คู่สัญญา และผู้ให้บริการภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษรหรือไม่	5	4	20	เสี่ยงสูง
2	องค์กรมีการแบ่งภารกิจและกำหนดผู้รับผิดชอบของหน่วยงานด้าน IT สารสนเทศในการควบคุมการเข้าถึงข้อมูลและทรัพย์สินสารสนเทศอย่างชัดเจนและเหมาะสมหรือไม่	5	5	25	เสี่ยงสูงมาก
3	องค์กรมีการระบุข้อตกลงการรักษาความลับข้อมูลสารสนเทศในเอกสารสัญญาจ้าง เอกสาร TOR ของโครงการด้านเทคโนโลยีสารสนเทศหรือไม่	4	4	16	สูง
4	องค์กรมีและใช้ข้อมูลที่เป็นปัจจุบันในการติดต่อแลกเปลี่ยนเรียนรู้ด้านเทคโนโลยีสารสนเทศภัยคุกคามหรือจุดอ่อนกับหน่วยงานที่มีความรอบรู้ ความชำนาญด้านความมั่นคงปลอดภัยหรือไม่	5	4	20	เสี่ยงสูง
5	องค์กรมีการกำหนดแนวทางการปฏิบัติงานจากระยะไกลเพื่อควบคุมการเข้าถึงการประมวลผล และจัดเก็บข้อมูลการใช้งานหรือไม่	4	5	20	เสี่ยงสูง

ตาราง 11 (ต่อ) แสดงด้านที่ 2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
6	องค์กรมีการกำหนดนโยบายถึงแนวทางปฏิบัติสำหรับการใช้งานอุปกรณ์สื่อสารแบบพกพาโดยมีการแจ้งให้บุคลกรภายในและหน่วยงานภายนอกที่เกี่ยวข้องรับทราบหรือไม่	5	5	25	เสี่ยงสูงมาก

จากตางราง 11 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่า ด้านที่ 2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อที่มี **ระดับความเสี่ยงสูงมาก** ได้แก่ ข้อ 2 องค์กรมีการแบ่งภารกิจและกำหนดผู้รับผิดชอบของหน่วยงานด้าน IT สารสนเทศในการควบคุมการเข้าถึงข้อมูลและทรัพย์สินสารสนเทศอย่างชัดเจนและเหมาะสมหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 และข้อ 6 องค์กรมีการกำหนดนโยบายถึงแนวทางปฏิบัติสำหรับการใช้งานอุปกรณ์สื่อสารแบบพกพาโดยมีการแจ้งให้บุคลกรภายในและหน่วยงานภายนอกที่เกี่ยวข้องรับทราบหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมา **ระดับความเสี่ยงสูง** ได้แก่ ข้อ 1 องค์กรมีการกำหนดขอบเขตและมอบหมายหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศให้แก่พนักงานภายในองค์กร คู่สัญญา และผู้ให้บริการภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษรหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 4 องค์กรมีและใช้ข้อมูลที่เป็นปัจจุบันในการติดต่อแลกเปลี่ยนเรียนรู้ด้านเทคโนโลยีสารสนเทศภัยคุกคามหรือจุดอ่อนกับหน่วยงานที่มีความรอบรู้ ความชำนาญ ด้านความมั่นคงปลอดภัยหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20ข้อ 5 องค์กรมีการกำหนดแนวทางการปฏิบัติงานจากระยะไกลเพื่อควบคุมการเข้าถึงการประมวลผล และจัดเก็บข้อมูลการใช้งานหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 และข้อ 3 องค์กรมีการระบุข้อตกลงการรักษาความลับข้อมูลสารสนเทศในเอกสารสัญญาจ้างเอกสาร TOR ของโครงการด้านเทคโนโลยีสารสนเทศหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 16

ตาราง 12 แสดงด้านที่ 3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีการจัดเก็บข้อมูลบุคลากรโดยใช้ระบบเทคโนโลยีสารสนเทศและมีนโยบาย ระเบียบ ข้อบังคับในการตรวจสอบประวัติการทำงานย้อนหลังก่อนรับสมัครบุคลากรเข้าทำงานในองค์กรหรือไม่	5	4	20	เสี่ยงสูง
2	องค์กรมีการกำหนดข้อตกลงในการจ้างงานที่ระบุให้ผู้รับจ้างปฏิบัติตามกฎระเบียบ และความรับผิดชอบด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรหรือไม่	4	4	16	สูง
3	องค์กรมีการกำหนดให้บุคลากรในองค์กรปฏิบัติตามนโนบายด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและมีการกำกับดูแลตามสายบังคับบัญชาหรือไม่	4	4	16	สูง
4	องค์กรมีการจัดฝึกอบรมเพื่อสร้างความตระหนัก รับรู้ เกี่ยวกับความมั่นคงปลอดภัยจากการใช้งานสารสนเทศและกระบวนการปฏิบัติงานอย่างสม่ำเสมอหรือไม่	5	5	25	เสี่ยงสูงมาก
5	องค์กรมีระบบการตรวจสอบและระบุทลงโทษทางวินัย หากมีการละเมิดหรือกระทำที่ทำให้องค์กรเกิดความเสี่ยงความเสียหายต่อความมั่นคงปลอดภัยจากการใช้งานสารสนเทศหรือไม่	5	5	25	เสี่ยงสูงมาก

ตาราง 12 (ต่อ) แสดงด้านที่ 3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
6	องค์กรมีการกำหนดขั้นตอนการปฏิบัติด้านความมั่นคงปลอดภัยเมื่อพนักงานสิ้นสุดการจ้างหรือเปลี่ยนแปลงตำแหน่งงาน และได้มีการดำเนินการตามนั้นหรือไม่	5	5	25	เสี่ยงสูงมาก

จากตางราง 12 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่า ด้านที่ 3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร ข้อที่มี **ระดับความเสี่ยงสูงมาก** ได้แก่ ข้อ 4 องค์กรมีการจัดฝึกอบรมเพื่อสร้างความตระหนัก รับรู้ เกี่ยวกับความมั่นคงปลอดภัยจากการใช้งานสารสนเทศและกระบวนการปฏิบัติงานอย่างสม่ำเสมอหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 ข้อ 5 องค์กรมีระบบการตรวจสอบและระบุบทลงโทษ ทางวินัยหากมีการละเมิดหรือกระทำที่ทำให้องค์กรเกิดความเสี่ยง ความเสียหายต่อความมั่นคงปลอดภัยจากการใช้งานสารสนเทศหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 และข้อ 6 องค์กรมีการกำหนดขั้นตอนการปฏิบัติด้านความมั่นคงปลอดภัย เมื่อพนักงานสิ้นสุดการจ้างหรือเปลี่ยนแปลงตำแหน่งงาน และได้มีการดำเนินการตามนั้นหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมา **ระดับความเสี่ยงสูง** ได้แก่ ข้อ 1 องค์กรมีการจัดเก็บข้อมูลบุคลากรโดยใช้ระบบเทคโนโลยีสารสนเทศ และมีนโยบาย ระเบียบ ข้อบังคับในการตรวจสอบประวัติการทำงานย้อนหลังก่อนรับสมัครบุคลากรเข้าทำงานในองค์กรหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 2 องค์กรมีการกำหนดข้อตกลงในการจ้างงานที่ระบุให้ผู้รับจ้างปฏิบัติตามกฎระเบียบ และความรับผิดชอบด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 16และข้อ 3 องค์กรมีการกำหนดให้บุคลากรในองค์กรปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและมีการกำกับดูแลตามสายบังคับบัญชาหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 16

ตาราง 13 แสดงด้านที่ 4 การบริหารจัดการทรัพย์สินสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีการจัดทำบัญชีทรัพย์สินที่เกี่ยวข้องกับสารสนเทศหรือการประมวลผลสารสนเทศอย่างครบถ้วนและเป็นปัจจุบันหรือไม่	4	5	20	เสี่ยงสูง
2	รายการทรัพย์สินสารสนเทศองค์กรของท่านทุกรายการมีการระบุสถานที่จัดเก็บและผู้รับผิดชอบที่ชัดเจนหรือไม่	5	5	25	เสี่ยงสูงมาก
3	องค์กรมีการกำหนดให้พนักงานคืนทรัพย์สินทั้งหมดที่ถือครองเมื่อสิ้นสุดการจ้างงานหรือเปลี่ยนแปลงตำแหน่งงานและตรวจสอบความครบถ้วนในทรัพย์สินนั้นหรือไม่	5	4	20	เสี่ยงสูง
4	องค์กรมีนโยบายในการจัดชั้นความลับของข้อมูลและกำหนดขั้นตอนการปฏิบัติงานตามระดับชั้นความลับหรือไม่	5	4	20	เสี่ยงสูง
5	องค์กรมีการกำหนดขั้นตอนปฏิบัติการจัดการและจัดเก็บสารสนเทศได้อย่างเหมาะสมสอดคล้องกับประเภทของสารสนเทศหรือไม่	4	4	16	เสี่ยงสูง
6	องค์กรมีการกำหนดขั้นตอนการปฏิบัติและการทำลายข้อมูลในอุปกรณ์บันทึกข้อมูลได้อย่างเหมาะสมและสอดคล้องกับประเภทของสารสนเทศหรือไม่	5	5	25	เสี่ยงสูงมาก

ตาราง 13 (ต่อ) แสดงด้านที่ 4 การบริหารจัดการทรัพย์สินสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
7	องค์กรมีการสำรองอุปกรณ์ประมวลผลสารสนเทศไว้อย่างเพียงพอตรงตามความต้องการและพร้อมใช้งานหรือไม่	4	5	20	เสี่ยงสูง

จากตางราง 13 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่า ด้านที่ 4 การบริหารจัดการทรัพย์สินสารสนเทศ ข้อที่มี **ระดับความเสี่ยงสูงมาก** ได้แก่ ข้อ 2 รายการทรัพย์สินสารสนเทศองค์กรของท่านทุกรายการมีการระบุสถานที่จัดเก็บและผู้รับผิดชอบที่ชัดเจนหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 และข้อ 6 องค์กรมีการกำหนดขั้นตอนการปฏิบัติและการทำลายข้อมูลในอุปกรณ์บันทึกข้อมูลได้อย่างเหมาะสมและสอดคล้องกับประเภท ของสารสนเทศหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมา **ระดับความเสี่ยงสูง** ได้แก่ ข้อ 1 องค์กรมีการจัดทำบัญชีทรัพย์สินที่เกี่ยวข้องกับสารสนเทศหรือการประมวลผลสารสนเทศอย่างครบถ้วนและเป็นปัจจุบันหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 3 องค์กรมีการกำหนดให้พนักงานคืนทรัพย์สินทั้งหมดที่ถือครองเมื่อสิ้นสุดการจ้างงานหรือเปลี่ยนแปลงตำแหน่งงานและตรวจสอบความครบถ้วนในทรัพย์สินนั้นหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 4 องค์กรมีนโยบายในการจัดชั้นความลับของข้อมูลและกำหนดขั้นตอนการปฏิบัติงานตามระดับชั้นความลับหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 7 องค์กรมีการสำรองอุปกรณ์ประมวลผลสารสนเทศไว้อย่างเพียงพอตรงตามความต้องการและพร้อมใช้งานหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 และข้อ 5 องค์กรมีการกำหนดขั้นตอนปฏิบัติการจัดการและจัดเก็บสารสนเทศได้อย่างเหมาะสม สอดคล้องกับประเภทของสารสนเทศหรือไม่มีค่าระดับความเสี่ยงอยู่ที่ 16

ตาราง 14 แสดงด้านที่ 5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีการจัดทำนโยบายควบคุมการเข้าถึงเครือข่ายอย่างเหมาะสม และมีการทบทวนสิทธิ์อย่างสม่ำเสมอหรือไม่ เช่น การบริหารจัดการรหัสผ่าน การพิสูจน์ตัวตนและการเข้าถึงศูนย์คอมพิวเตอร์ เป็นต้น	4	4	16	สูง
2	องค์กรมีการกำหนดให้ผู้ใช้งานภายนอกสามารถเข้าถึงเครือข่ายและการบริการเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น และทุกครั้งต้องมีการลงทะเบียนขอสิทธิการเข้าถึงเครือข่ายหรือไม่	4	4	16	สูง
3	องค์กรกำหนดขั้นตอนปฏิบัติการลงทะเบียนผู้ใช้งานใหม่และขั้นตอนการถอดถอนสิทธิ์การใช้งานเมื่อออกจากองค์กรหรือไม่	5	5	25	เสี่ยงสูงมาก
4	องค์มีการกำหนดระดับสิทธิ์การเข้าถึงระบบงาน ระบบปฏิบัติการ ระบบฐานข้อมูล หรือระบบงานอื่น ๆ เหมาะสมต่อความจำเป็นของผู้ใช้งานแต่ละตำแหน่งหรือไม่	4	5	20	เสี่ยงสูง
5	องค์กรมีการอบรมให้ความรู้แนวทางการกำหนดรหัสผ่านเกี่ยวกับการใช้งานด้านเทคโนโลยีสารสนเทศที่ปลอดภัยให้แก่บุคลากรในองค์กรหรือไม่	5	5	25	เสี่ยงสูงมาก

ตาราง 14 (ต่อ) แสดงด้านที่ 5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
6	องค์กรมีการกำหนดระยะเวลาสิ้นสุดการใช้งานของระบบงานเมื่อไม่มีกิจกรรมหรือมีการกำหนดระยะเวลาในการเชื่อมต่อระบบงานหรือไม่	4	5	20	เสี่ยงสูง
7	องค์กรมีนโยบายการตรวจสอบควบคุมการใช้งานโปรแกรมอรรถประโยชน์นอกเหนือจากที่องค์กรกำหนดหรือไม่	5	5	25	เสี่ยงสูงมาก

จากตางราง 16 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่า ด้านที่ 5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ ข้อที่มี **ระดับความเสี่ยงสูงมาก** ได้แก่ ข้อ 3 องค์กรกำหนดขั้นตอนปฏิบัติการลงทะเบียนผู้ใช้งานใหม่และขั้นตอนการถอดถอนสิทธิ์การใช้งานเมื่อออกจากองค์กรหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 ข้อ 5 องค์กรมีการอบรมให้ความรู้แนวทางการกำหนดรหัสผ่านเกี่ยวกับการใช้งานด้านเทคโนโลยีสารสนเทศที่ปลอดภัยให้แก่บุคลากรในองค์กรหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 และข้อ 7 องค์กรมีนโยบายการตรวจสอบควบคุมการใช้งานโปรแกรมอรรถประโยชน์นอกเหนือจากที่องค์กรกำหนดหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมา **ระดับความเสี่ยงสูง** ได้แก่ ข้อ 4 องค์มีการกำหนดระดับสิทธิ์การเข้าถึงระบบงาน ระบบปฏิบัติการ ระบบฐานข้อมูล หรือระบบงานอื่น ๆ เหมาะสมต่อความจำเป็นของผู้ใช้งานแต่ละตำแหน่งหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 และข้อ 6 องค์กรมีการกำหนดระยะเวลาสิ้นสุดการใช้งานของระบบงานเมื่อไม่มีกิจกรรมหรือมีการกำหนดระยะเวลาในการเชื่อมต่อระบบงานหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 1 องค์กรมีการจัดทำนโยบายควบคุมการเข้าถึงเครือข่ายอย่างเหมาะสม และมีการทบทวนสิทธิ์อย่างสม่ำเสมอหรือไม่ เช่น การบริหารจัดการรหัสผ่าน การพิสูจน์ตัวตน และการเข้าถึงศูนย์คอมพิวเตอร์ เป็นต้น มีค่าระดับความเสี่ยงอยู่ที่ 16 และองค์กรมีการกำหนดให้ผู้ใช้งานภายนอกสามารถ

เข้าถึงเครือข่ายและการบริการเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น และทุกครั้งต้องมีการลงทะเบียนขอสิทธิการเข้าถึงเครือข่ายหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 16

ตาราง 15 แสดงด้านที่ 6 การควบคุมการเข้ารหัสข้อมูล

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีการกำหนดนโยบายการเข้าใช้งานรหัสข้อมูล และมีการตรวจสอบการใช้งานตามนโยบายหรือไม่	5	5	25	เสี่ยงสูงมาก

จากตางราง 15 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่า ด้านที่ 6 การควบคุมการเข้ารหัสข้อมูล ข้อที่มี **ระดับความเสี่ยงสูงมาก** ได้แก่ ข้อ 1 องค์กรมีการกำหนดนโยบายการเข้าใช้งานรหัสข้อมูล และมีการตรวจสอบการใช้งานตามนโยบายหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25

ตาราง 16 แสดงด้านที่ 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีการกำหนดขอบเขตหรือบริเวณโดยรอบทางกายภาพที่ต้องมีการรักษาความมั่นคงปลอดภัย การแบ่งแยกพื้นที่เหมาะสมหรือไม่	4	5	20	เสี่ยงสูง
2	องค์กรมีการควบคุมการเข้าออกของพื้นที่เฉพาะผู้ที่มีสิทธิ์หรือผู้ที่ได้รับอนุญาตและได้มีการจัดทำขั้นตอนปฏิบัติสำหรับเข้าออกศูนย์คอมพิวเตอร์ศูนย์สารสนเทศ กทั้งวิธีการสื่อสารถึงผู้ที่เกี่ยวข้อง?	5	4	20	เสี่ยงสูง

ตาราง 16 (ต่อ) แสดงด้านที่ 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
3	องค์กรมีการออกแบบการรักษาความมั่นคงปลอดภัยทางกายภาพของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวก หน่วยงานสารสนเทศ และศูนย์คอมพิวเตอร์ หรือไม่ เช่น มี Access Control หรือกล้องวงจรปิด เป็นต้น	5	5	25	เสี่ยงสูงมาก
4	องค์กรมีการมีการป้องกันภัยทางธรรมชาติการโจมตีหรือการบุกรุกจากภายนอก อุบัติเหตุที่เหมาะสมและมีการตรวจสอบการใช้งานอย่างสม่ำเสมอหรือไม่ เช่น มีการติดตั้ง Fire Alarm, Air Condition, Smoke Detector, เครื่องตรวจวัดความชื้น, ถังดับเพลิง เป็นต้น	5	3	15	ปานกลาง
5	องค์กรมีการจัดวางอุปกรณ์สารสนเทศได้อย่างเหมาะสมปลอดภัย และกำหนดให้ผู้มีสิทธิ์เท่านั้นที่สามารถเข้าถึงอุปกรณ์ได้อย่างเหมาะสมหรือไม่ เช่น ติดตั้งอุปกรณ์ในตู้ Rack และมีผู้รับผิดชอบกุญแจตู้ Rack เป็นต้น	4	3	12	ปานกลาง

ตาราง 16 (ต่อ) แสดงด้านที่ 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
6	องค์กรมีการป้องกันการหยุดชะงักของอุปกรณ์ขณะทำงาน เช่น มีการติดตั้ง UPS สำรองไฟ ระบบควบคุมอุณหภูมิ และเครื่องกำเนิดไฟฟ้า เป็นต้น ในแต่ละส่วนงานหรือไม่	5	4	20	เสี่ยงสูง
7	องค์กรมีการจัด ทำ Label และจัดระเบียบ สายไฟ สายสื่อสาร และสายเคเบิ้ล เพื่อไม่ก่อให้เกิดการขัดขวางการทำงาน ป้องกันการแทรกแซงสัญญาณหรือการทำให้เสียหายหรือไม่	5	3	15	ปานกลาง
8	องค์กรมีการกำหนดขั้นตอนการปฏิบัติรักษาความปลอดภัยทรัพย์สินที่นำไปใช้งานนอกองค์กรหรือไม่	4	3	12	ปานกลาง
9	องค์กรมีการกำหนดมาตรการป้องกันอุปกรณ์ ในขณะที่ไม่มีผู้ดูแลหรือการใช้งานหรือไม่ เช่น มีการปิดหน้าจอและกำหนดการเข้ารหัสในการใช้งาน เป็นต้น	5	4	20	เสี่ยงสูง

จากตางราง 16 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่า ด้านที่ 7

การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ข้อที่มี **ระดับความเสี่ยงสูงมาก** ได้แก่ ข้อ 3 องค์กรมีการออกแบบการรักษาความมั่นคงปลอดภัย ทางกายภาพของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวก หน่วยงานสารสนเทศ และศูนย์คอมพิวเตอร์ หรือไม่ เช่น มี Access Control หรือกล้องวงจรปิด เป็นต้น มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมา **ระดับความเสี่ยงสูง** ได้แก่ ข้อ 1 องค์กรมีการกำหนดขอบเขตหรือบริเวณโดยรอบทางกายภาพที่ต้องมีการรักษาความมั่นคงปลอดภัย การแบ่งแยกพื้นที่เหมาะสมหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 2 องค์กรมีการควบคุมการเข้าออกของพื้นที่เฉพาะผู้ที่มีสิทธิ์หรือผู้ที่ได้รับอนุญาต และได้มีการจัดทำขั้นตอนปฏิบัติสำหรับเข้าออกศูนย์คอมพิวเตอร์ ศูนย์สารสนเทศอีกทั้งวิธีการสื่อสารถึงผู้ที่เกี่ยวข้องหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 6 องค์กรมีการป้องกันการหยุดชะงักของอุปกรณ์ขณะทำงาน เช่น มีการติดตั้ง UPS สำรองไฟ ระบบควบคุมอุณหภูมิ และเครื่องกำเนิดไฟฟ้า เป็นต้น ในแต่ละส่วนงานหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 และข้อ 9 องค์กรมีการกำหนดมาตรการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ดูแลหรือการใช้งานหรือไม่ เช่น มีการปิดหน้าจอและกำหนดการเข้ารหัสในการใช้งาน เป็นต้น มีค่าระดับความเสี่ยงอยู่ที่ 20 สำหรับ **ระดับความเสี่ยงปานกลาง** ได้แก่ ข้อ 4 องค์กรมีการป้องกันภัยทางธรรมชาติการโจมตีหรือการบุกรุกจากภายนอก อุบัติเหตุที่เหมาะสมและมีการตรวจสอบการใช้งานอย่างสม่ำเสมอหรือไม่ เช่น มีการติดตั้ง Fire Alarm, Air Condition, Smoke Detector,เครื่องตรวจวัดความชื้น, ถังดับเพลิง เป็นต้น มีค่าระดับความเสี่ยงอยู่ที่ 15 ข้อ 7 องค์กรมีการจัดทำ Label และจัดระเบียบ สายไฟ สายสื่อสารและสายเคเบิ้ล เพื่อไม่ก่อให้เกิดการขัดขวางการทำงาน ป้องกันการแทรกแซงสัญญาณหรือการทำให้เสียหายหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 15 ข้อ 5 องค์กรมีการจัดวางอุปกรณ์สารสนเทศได้อย่างเหมาะสม ปลอดภัย และกำหนดให้ผู้มีสิทธิ์เท่านั้นที่สามารถเข้าถึงอุปกรณ์ได้อย่างเหมาะสมหรือไม่ เช่น ติดตั้งอุปกรณ์ในตู้ Rackและมีผู้รับผิดชอบกุญแจตู้ Rack เป็นต้น มีค่าระดับความเสี่ยงอยู่ที่ 12 และ ข้อ 8 องค์กรมีการกำหนดขั้นตอนการปฏิบัติ รักษาความปลอดภัยทรัพย์สินที่นำไปใช้งานนอกองค์กรหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 12

ตาราง 17 แสดงด้านที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีการกำหนดขั้นตอน	5	4	20	เสี่ยงสูง

ปฏิบัติงานที่เกี่ยวข้องกับระบบ

ตาราง 17 (ต่อ) แสดงด้านที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
	เทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรและเป็นปัจจุบันหรือไม่ เช่น ขั้นตอนการปฏิบัติงานในศูนย์คอมพิวเตอร์ การสำรองข้อมูลการนำเข้าข้อมูลระบบในงาน การกู้คืนระบบ เป็นต้น				
2	องค์กรมีการตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ตั้งโต๊ะของบุคลากรในองค์กรหรือไม่ ว่ามีการติดตั้ง Anti-virus และตั้ง Auto Update รวมถึงการสร้างความตระหนักในการจัดการโปรแกรมไม่ประสงค์ดี	4	4	16	สูง
3	องค์กรมีการกำหนดขั้นตอนการสำรองข้อมูลและรายงานผลการทดสอบข้อมูลที่สำรองต่อผู้บังคับบัญชาอย่างสม่ำเสมอหรือไม่	5	5	25	เสี่ยงสูงมาก
4	องค์กรมีการกำหนดสิทธิการเข้าถึงอุปกรณ์บันทึกล็อคเฉพาะผู้มีสิทธิ์หรือไม่	5	3	15	ปานกลาง
5	องค์กรมีการตั้งเวลาของระบบที่สำคัญทั้งหมดในองค์กรว่าถูกต้องตรงกันกับอุปกรณ์เทียบเวลาจาก	4	5	20	เสี่ยงสูง

แหล่งอ้างอิง NTP Server หรือไม่

ตาราง 17 (ต่อ) แสดงด้านที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
6	องค์กรมีการติดตาม เฝ้าระวัง และประเมินความเสี่ยงช่องโหว่ที่เกิดขึ้น และมีมาตรการจัดการช่องโหวที่เกิดขึ้นอย่างเหมาะสม ทันเวลาหรือไม่	5	4	20	เสี่ยงสูง
7	องค์กรมีการตรวจสอบควบคุมการติดตั้งซอฟต์แวร์ ว่ามีความเหมาะสมและเป็นปัจจุบันหรือไม่	5	4	20	เสี่ยงสูง

จากตางราง 17 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่า ด้านที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ ข้อที่มี **ระดับความเสี่ยงสูงมาก** ได้แก่ ข้อ 3 องค์กรมีการกำหนดขั้นตอนการสำรองข้อมูลและรายงานผลการทดสอบข้อมูลที่สำรองต่อผู้บังคับบัญชาอย่างสม่ำเสมอหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมา **ระดับความเสี่ยงสูง** ได้แก่ ข้อ 1 องค์กรมีการกำหนดขั้นตอนปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรและเป็นปัจจุบันหรือไม่ เช่น ขั้นตอนการปฏิบัติงานในศูนย์คอมพิวเตอร์ การสำรองข้อมูลการนำเข้าข้อมูลระบบในงานการกู้คืนระบบ เป็นต้น มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 5 องค์กรมีการตั้งเวลาของระบบที่สำคัญทั้งหมดในองค์กรว่าถูกต้อง ตรงกันกับอุปกรณ์เทียบเวลาจากแหล่งอ้างอิง NTP Server หรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 6 องค์กรมีการติดตาม เฝ้าระวัง และประเมินความเสี่ยงช่องโหว่ที่เกิดขึ้น และมีมาตรการจัดการช่องโหวที่เกิดขึ้นอย่างเหมาะสม ทันเวลาหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 7 องค์กรมีการตรวจสอบควบคุมการติดตั้งซอฟต์แวร์ ว่ามีความเหมาะสมและเป็นปัจจุบันหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 และข้อ 2 องค์กรมีการตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ตั้งโต๊ะของบุคลากรในองค์กรหรือไม่ ว่ามีการติดตั้ง Anti-virus และตั้ง Auto Update รวมถึงการสร้าง

ความตระหนักในการจัดการโปรแกรมไม่ประสงค์ดี มีค่าระดับความเสี่ยงอยู่ที่ 16 สำหรับ **ระดับความเสี่ยงปานกลาง** ได้แก่ ข้อ 4 องค์กรมีการกำหนดสิทธิการเข้าถึงอุปกรณ์บันทึกล็อคเฉพาะผู้มีสิทธิ์หรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 15

ตาราง 18 แสดงด้านที่ 9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสาร

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีการบริหารจัดการควบคุมเครือข่ายโดยแบ่งแยกโซนเครือข่าย และแบ่งแยก VLAN กลุ่มผู้ใช้งานหรือไม่	5	5	25	เสี่ยงสูงมาก
2	องค์กรมีการกำหนดระดับของข้อตกลงในการให้บริการเครือข่ายไว้อย่างเหมาะสมทั้งการให้บริการภายในและภายนอกองค์กรหรือไม่	5	4	20	เสี่ยงสูง
3	องค์กรมีการกำหนดนโยบาย ขั้นตอนการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานภายนอกตลอดจนการรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูลสารสนเทศขององค์กรกับหน่วยงานภายนอกหรือไม่	5	5	25	เสี่ยงสูงมาก

จากตางราง 20 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่า ด้านที่ 9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ ข้อที่มี **ระดับความเสี่ยงสูงมาก** ได้แก่ ข้อ 1 องค์กรมีการบริหารจัดการควบคุมเครือข่าย โดยแบ่งแยกโซนเครือข่าย และแบ่งแยก VLAN กลุ่มผู้ใช้งานหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 และข้อ 3 องค์กรมีการกำหนดนโยบาย ขั้นตอนการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงาน

ภายนอกตลอดจนการรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูลสารสนเทศขององค์กรกับหน่วยงานภายนอกหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมา **ระดับความเสี่ยงสูง** ได้แก่ ข้อ 2 องค์กรมีการกำหนดระดับของข้อตกลงในการให้บริการเครือข่ายไว้อย่างเหมาะสมทั้งการให้บริการภายในและภายนอกองค์กรหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20

ตาราง 19 แสดงด้านที่ 10 การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีกระบวนการป้องกันข้อมูลสารสนเทศจากการถูกเปิดเผยหรือเปลี่ยนแปลงแก้ไขข้อมูลโดยผู้ที่ไม่มีสิทธิ รวมถึงมีการวิเคราะห์ช่องโหว่หรือการทดสอบเจาะระบบการส่งข้อมูลผ่านเครือข่ายสาธารณะหรือไม่	5	4	20	เสี่ยงสูง
2	องค์กรมีกระบวนการป้องกันข้อมูลสารสนเทศบนธุรกรรมออนไลน์จากการรับส่งข้อมูลที่ไม่สมบูรณ์ ผิดเส้นทาง หรือมีการเปลี่ยนแก้ไขจากผู้ที่ไม่มีสิทธิหรือไม่	5	5	25	เสี่ยงสูงมาก
3	องค์กรมีการกำหนดข้อตกลงในการพัฒนาระบบให้มีความมั่นคงปลอดภัย และมีการตรวจสอบว่ามีการปฏิบัติตามข้อตกลงหรือไม่	4	4	16	สูง
4	องค์กรมีแนวทางการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ รวมถึงมีการทดสอบหลังการเปลี่ยนแปลง	5	4	20	เสี่ยงสูง

ตาราง 19 (ต่อ) แสดงด้านที่ 10 การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
	โดยได้รับการอนุมัติให้มีการประเมินผลกระทบจากผู้มีอำนาจและมีการรายงานผลทุกครั้งหรือไม่				
5	องค์กรมีการกำหนดหลักวิศวกรรมระบบให้มีความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษรและเป็นปัจจุบันหรือไม่	5	3	15	ปานกลาง

จากตางราง 19 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่า ด้านที่ 10 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ ข้อที่มี **ระดับความเสี่ยงสูงมาก** ได้แก่ ข้อ 2 องค์กรมีกระบวนการป้องกันข้อมูลสารสนเทศบนธุรกรรมออนไลน์จากการรับส่งข้อมูลที่ไม่สมบูรณ์ ผิดเส้นทาง หรือมีการเปลี่ยนแก้ไขจากผู้ที่ ไม่มีสิทธิหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมา **ระดับความเสี่ยงสูง** ได้แก่ ข้อ 1 องค์กรมีกระบวนการป้องกันข้อมูลสารสนเทศจากการถูกเปิดเผยหรือเปลี่ยนแปลงแก้ไขข้อมูลโดยผู้ที่ไม่มีสิทธิ รวมถึงมีการวิเคราะห์ช่องโหว่หรือการทดสอบเจาะระบบการส่งข้อมูลผ่านเครือข่ายสาธารณะหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 4 องค์กรมีแนวทางการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ รวมถึงมีการทดสอบหลังการเปลี่ยนแปลง โดยได้รับการอนุมัติให้มีการประเมินผลกระทบจากผู้มีอำนาจและมีการรายงานผลทุกครั้งหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 และข้อ 3 องค์กรมีการกำหนดข้อตกลงในการพัฒนาระบบให้มีความมั่นคงปลอดภัย และมีการตรวจสอบว่ามีการปฏิบัติตามข้อตกลงหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 16 สำหรับ **ระดับความเสี่ยงปานกลาง** ได้แก่ ข้อ 5 องค์กรมีการกำหนดหลักวิศวกรรมระบบให้มีความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษรและเป็นปัจจุบันหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 15

ตาราง 20 แสดงด้านที่ 11 การควบคุมดูแลผู้ให้บริการภายนอก

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีแนวทางปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศระหว่างองค์กรกับผู้ให้บริการภายนอกหรือไม่ เช่น การกำหนดสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก เป็นต้น	5	5	25	เสี่ยงสูงมาก
2	องค์กรมีการทำสัญญาจ้างกับผู้ให้บริการภายนอก โดยมีข้อกำหนดในการควบคุมการดำเนินงานของผู้ให้บริการภายนอกและผู้ที่เกี่ยวข้องต้องปฏิบัติตามข้อกำหนดขององค์กรหรือไม่	5	4	20	เสี่ยงสูง
3	องค์กรมีการติดตามและทบทวนการให้บริการของผู้ให้บริการภายนอก โดยมีการประเมินผลการให้บริการและรายงานแก่หัวหน้าหรือผู้บังคับบัญชาหรือไม่	5	5	25	เสี่ยงสูงมาก

จากตาราง 20 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่า ด้านที่ 11 การควบคุมดูแลผู้ให้บริการภายนอก ข้อที่มี **ระดับความเสี่ยงสูงมาก** ได้แก่ ข้อ 1 องค์กรมีแนวทางปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศระหว่างองค์กรกับผู้ให้บริการภายนอกหรือไม่ เช่น การกำหนดสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการ

ภายนอก เป็นต้น มีค่าระดับความเสี่ยงอยู่ที่ 25 และข้อ 3 องค์กรมีการติดตามและทบทวนการให้บริการของผู้ให้บริการภายนอก โดยมีการประเมินผลการให้บริการและรายงานแก่หัวหน้าหรือผู้บังคับบัญชาหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมา **ระดับความเสี่ยงสูง** ได้แก่ข้อ 2 องค์กรมีการทำสัญญาจ้างกับผู้ให้บริการภายนอก โดยมีข้อกำหนดในการควบคุมการดำเนินงานของผู้ให้บริการภายนอกและผู้ที่เกี่ยวข้องต้องปฏิบัติตามข้อกำหนดขององค์กรหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20

ตาราง 21 แสดงด้านที่ 12 การบริหารจัดการเหตุการณ์

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีการกำหนดขั้นตอนการรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมหรือไม่	5	4	20	เสี่ยงสูง
2	องค์กรมีการกำหนดเกณฑ์ประเมินสถานการณ์ความมั่นคงปลอดภัยจากเหตุการณ์ที่ไม่พึงประสงค์และวิธีแก้ไขเหตุขัดข้องหรือไม่	4	4	16	เสี่ยงสูง
3	องค์กรมีการจัดทำสรุปจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยเพื่อหาแนวทางในการแก้ไขระยะยาวหรือไม่	5	5	25	เสี่ยงสูงมาก
4	องค์กรมีการกำหนดแนวทางการระบุ รวบรวม จัดหาและจัดเก็บหลักฐานข้อมูลสารสนเทศเมื่อเกิดเหตุการณ์ที่มีความเกี่ยวข้องกับการดำเนินการทางกฎหมายหรือไม่	4	5	20	เสี่ยงสูง

จากตางราง 21 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่า ด้านที่ 12 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อที่มี **ระดับความเสี่ยงสูงมาก** ได้แก่ ข้อ 3 องค์กรมีการจัดทำสรุปจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยเพื่อหาแนวทางในการแก้ไขระยะยาวหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมา **ระดับความเสี่ยงสูง** ได้แก่ ข้อ 1 องค์กรมีการกำหนดขั้นตอนการรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 และข้อ 4 องค์กรมีการกำหนดแนวทางการระบุ รวบรวม จัดหาและจัดเก็บหลักฐานข้อมูลสารสนเทศเมื่อเกิดเหตุการณ์ที่มีความเกี่ยวข้องกับการดำเนินการทางกฎหมายหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20 และข้อ 2 องค์กรมีการกำหนดเกณฑ์ประเมินสถานการณ์ความมั่นคงปลอดภัยจากเหตุการณ์ที่ไม่พึงประสงค์และวิธีแก้ไขเหตุขัดข้องหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20

ตาราง 22 แสดงด้านที่ 13 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีข้อกำหนดสำหรับความมั่นคงปลอดภัยสารสนเทศและความต่อเนื่องสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในสถานการณ์ร้ายแรงหรือไม่ เช่น การวางแผนเตรียมการสภาพความพร้อมใช้ของระบบงานในนโยบายว่ามีการประเมินผลกระทบทางธุรกิจกรณีระบบงานหยุดชะงักและกำหนดระดับความสำคัญของระบบงานหรือไม่	5	3	15	ปานกลาง

ตาราง 22 (ต่อ) แสดงด้านที่ 13 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
2	องค์กรมีการเตรียมสำรองอุปกรณ์ประมวลผลสารสนเทศไว้อย่างเพียงพอตรงตามความต้องการ และมีความพร้อมใช้งาน ได้รับการบำรุงรักษาอย่างเหมาะสม และมีสำรองกรณี ชำรุดเสียหายไม่สามารถซ่อมได้หรือไม่	3	3	9	เสี่ยงต่ำ

จากตางราง 22 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่า ด้านที่ 13 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อที่มี **ระดับความเสี่ยงปานกลาง** ได้แก่ ข้อ 1 องค์กรมีข้อกำหนดสำหรับความมั่นคงปลอดภัยสารสนเทศและความต่อเนื่องสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในสถานการณ์ร้ายแรงหรือไม่ เช่น การวางแผนเตรียมการสภาพความพร้อมใช้ของระบบงานในนโยบายว่ามีการประเมินผลกระทบทางธุรกิจกรณีระบบงานหยุดชะงักและกำหนดระดับความสำคัญของระบบงานหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 15 รองลงมา คือ **ระดับความเสี่ยงต่ำ** ได้แก่ ข้อ 2 องค์กรมีการเตรียมสำรองอุปกรณ์ประมวลผลสารสนเทศไว้อย่างเพียงพอตรงตามความต้องการและมีความพร้อมใช้งานได้รับการบำรุงรักษาอย่างเหมาะสม และมีสำรองกรณีชำรุดเสียหายไม่สามารถซ่อมได้หรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 9

ตาราง 23 แสดงด้านที่ 14 การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	องค์กรมีการจัดทำรายการข้อกฎหมายด้านความมั่นคง	5	5	25	เสี่ยงสูงมาก

ตาราง 23 (ต่อ) แสดงด้านที่ 14 การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด

ข้อ	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
	ปลอดภัยสารสนเทศ รวมถึงข้อกำหนดขององค์กรที่ต้องปฏิบัติไว้เป็นลายลักษณ์อักษร และอัพเดตเป็นปัจจุบัน อีกทั้งได้มีการเผยแพร่ให้คนในองค์กรทราบอย่างทั่วถึงหรือไม่				
2	องค์กรมีการจัดทำขั้นตอนการปฏิบัติงานการจัดการลิขสิทธิ์ซอฟต์แวร์ และมีการบริหารจัดการลิขสิทธิ์ซอฟต์แวร์อย่างเหมาะสมหรือไม่	5	4	20	เสี่ยงสูง
3	องค์กรมีการจัดทำขั้นตอนการปฏิบัติงานการจัดระดับชั้นความลับของข้อมูล การทำป้ายแสดงระดับชั้นความลับและการจัดการสารสนเทศในนโยบายหรือไม่	5	5	25	เสี่ยงสูงมาก
4	องค์กรมีการทบทวนการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศโดยผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกเป็นประจำตามรอบระยะเวลาที่กำหนดหรือไม่	5	5	25	เสี่ยงสูงมาก
5	องค์กรมีการทบทวนโยบายความมั่นคงปลอดภัยสารสนเทศโดยการอ้างอิงมาตรฐาน ISO 27001 ฉบับปัจจุบันหรือไม่	5	4	20	เสี่ยงสูง

จากตางราง 23 แสดงผลการประเมินระดับความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร ประเภทกลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร พบว่า ด้านที่ 14 การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด ข้อที่มี **ระดับความเสี่ยงสูงมาก** ได้แก่ ข้อ 1 องค์กรมีการจัดทำรายการข้อกฎหมายด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงข้อกำหนดขององค์กรที่ต้องปฏิบัติไว้เป็นลายลักษณ์อักษร และอัพเดตเป็นปัจจุบัน อีกทั้งได้มีการเผยแพร่ให้คนในองค์กรทราบอย่างทั่วถึงหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 ข้อ 3 องค์กรมีการจัดทำขั้นตอนการปฏิบัติงานการจัดระดับชั้นความลับของข้อมูล การทำป้ายแสดงระดับชั้นความลับและการจัดการสารสนเทศในนโยบายหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 และข้อ 4 องค์กรมีการทบทวนการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศโดยผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกเป็นประจำตามรอบระยะเวลาที่กำหนดหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 25 รองลงมา **ระดับความเสี่ยงสูง** ได้แก่ ข้อ 2 องค์กรมีการจัดทำขั้นตอนการปฏิบัติงานการจัดการลิขสิทธิ์ซอฟต์แวร์ และมีการบริหารจัดการลิขสิทธิ์ซอฟต์แวร์อย่างเหมาะสมหรือไม่มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 5 องค์กรมีการทบทวนโยบายความมั่นคงปลอดภัยสารสนเทศโดยการอ้างอิงมาตรฐาน ISO 27001 ฉบับปัจจุบันหรือไม่ มีค่าระดับความเสี่ยงอยู่ที่ 20

3. ผลการประเมินระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กร ของกลุ่มผู้ใช้งาน สถานศึกษาในสังกัด สถาบันการอาชีวศึกษาภาคเหนือ 2 จำนวน 9 แห่ง แบ่งเป็นกลุ่มเจ้าหน้าที่ทั่วไปและกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร

ตาราง 24 แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มผู้ใช้งานทั่วไป สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 จำนวน 9 แห่ง

สถานศึกษา	โอกาส	C ผลกระทบ	ผล	โอกาส	I ผลกระทบ	ผล	โอกาส	A ผลกระทบ	ผล	ผลรวม	แปรผลระดับความเสี่ยง
1. วิทยาลัยเทคนิคเชียงราย	5	4	20	4	5	20	4	5	20	20	เสี่ยงสูง
2.วิทยาลัยอาชีวศึกษาเชียงราย	4	4	16	4	4	16	4	4	16	16	เสี่ยงสูง

ตาราง 24 (ต่อ) แสดงผลภาพรวมการประเมินระดับความเสี่ยงของกลุ่มผู้ใช้งานทั่วไป สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 จำนวน 9 แห่ง

สถานศึกษา	C			I			A			ผลรวม	แปรผลระดับความเสี่ยง
	โอกาส	ผลกระทบ	ผล	โอกาส	ผลกระทบ	ผล	โอกาส	ผลกระทบ	ผล		
3. วิทยาลัยเทคนิคกาญจนาภิเษกเชียงราย	5	4	20	4	5	20	5	5	25	22	เสี่ยงสูงมาก
4.วิทยาลัยเทคนิคพะเยา	5	5	25	5	5	25	5	5	25	25	เสี่ยงสูงมาก
5.วิทยาลัยเกษตรและเทคโนโลยีพะเยา	5	5	25	4	5	20	5	5	25	23	เสี่ยงสูงมาก
6. วิทยาลัยเทคนิคแพร่	3	4	12	3	4	12	4	4	16	13	ปานกลาง
7.วิทยาลัยอาชีวศึกษาแพร่	4	4	16	3	4	12	5	5	25	18	เสี่ยงสูง
8.วิทยาลัยเกษตรและเทคโนโลยีแพร่	5	5	25	5	5	25	5	5	25	25	เสี่ยงสูงมาก
9. วิทยาลัยเทคนิคน่าน	5	4	20	5	5	25	5	5	25	23	เสี่ยงสูง

จากตาราง 24 แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มผู้ใช้งานทั่วไป สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 จำนวน 9 แห่ง พบว่า สถานศึกษาที่มี**ระดับความเสี่ยงสูงมาก** ได้แก่ วิทยาลัยเทคนิคกาญจนาภิเษกเชียงราย วิทยาลัยเทคนิคพะเยา วิทยาลัยเกษตรและเทคโนโลยีพะเยา และวิทยาลัยเกษตรและเทคโนโลยีแพร่ **ระดับความเสี่ยงสูง** ได้แก่ วิทยาลัยเทคนิคเชียงราย วิทยาลัยอาชีวศึกษาเชียงราย วิทยาลัยอาชีวศึกษาแพร่ วิทยาลัยเทคนิคน่าน และสถานศึกษาที่มีระดับความเสี่ยง **ปานกลาง** ได้แก่ วิทยาลัยเทคนิคแพร่

ตาราง 25 แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยเทคนิคเชียงราย

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
2	การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
3	การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร	5	5	25	เสี่ยงสูงมาก
4	การบริหารจัดการทรัพย์สินสารสนเทศ	5	5	25	เสี่ยงสูงมาก
5	การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ	4	5	20	เสี่ยงสูง
6	การควบคุมการเข้ารหัสข้อมูล	4	5	20	เสี่ยงสูง
7	การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม	5	4	20	เสี่ยงสูง
8	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ	5	4	20	เสี่ยงสูง
9	การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์	5	5	25	เสี่ยงสูงมาก
10	การจัดหา พัฒนาและดูแล	5	4	20	เสี่ยงสูง

รักษาระบบสารสนเทศ

ตาราง 25 (ต่อ) แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยเทคนิคเชียงราย

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
11	การควบคุมดูแลผู้ให้บริการภายนอก	4	5	20	เสี่ยงสูง
12	การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
13	การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	5	4	20	เสี่ยงสูง
14	การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด	5	4	20	เสี่ยงสูง
	รวม			**20**	**เสี่ยงสูง**

จากตาราง 25 แสดงผลการประเมินระดับความเสี่ยง ของกลุ่มตัวอย่างประเภทเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร วิทยาลัยเทคนิคเชียงราย สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 พบว่า ระดับความเสี่ยงของวิทยาลัยเทคนิคเชียงราย อยู่ในเกณฑ์**ระดับเสี่ยงสูง** หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงสูงมาก** ได้แก่ ข้อ 1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร ข้อ 4 การบริหารจัดการทรัพย์สินสารสนเทศ ข้อ 9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ ข้อ 12 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ โดยมีค่าระดับความเสี่ยงอยู่ที่ 25 ข้อที่มี

เกณฑ์ความเสี่ยงอยู่ใน **ระดับเสี่ยงสูง** ได้แก่ 5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศข้อ 6 การควบคุมการเข้ารหัสข้อมูล ข้อ 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ข้อ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ ข้อ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ ข้อ 10 การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ ข้อ 11 การควบคุมดูแลผู้ให้บริการภายนอก ข้อ 13 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 14 การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด มีค่าระดับความเสี่ยงอยู่ที่ 20

ตาราง 26 แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยอาชีวศึกษาเชียงราย

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	4	4	16	เสี่ยงสูง
2	การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ	4	4	16	เสี่ยงสูง
3	การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร	4	5	20	เสี่ยงสูง
4	การบริหารจัดการทรัพย์สินสารสนเทศ	3	5	15	ปานกลาง
5	การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ	4	5	20	เสี่ยงสูง
6	การควบคุมการเข้ารหัสข้อมูล	4	5	20	เสี่ยงสูง
7	การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม	4	4	16	เสี่ยงสูง

ตาราง 26 (ต่อ) แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยอาชีวศึกษาเชียงราย

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
8	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ	4	4	16	เสี่ยงสูง
9	การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์	4	4	16	เสี่ยงสูงมาก
10	การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ	3	4	12	ปานกลาง
11	การควบคุมดูแลผู้ให้บริการภายนอก	3	5	15	ปานกลาง
12	การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	3	5	15	ปานกลาง
13	การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	4	4	16	เสี่ยงสูง
14	การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด	3	4	12	ปานกลาง
	รวม			**15**	**ปานกลาง**

จากตาราง 26 แสดงผลการประเมินระดับความเสี่ยง ของกลุ่มตัวอย่างประเภทเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร วิทยาลัยอาชีวศึกษาชียงราย สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 พบว่า ระดับความเสี่ยงของวิทยาลัยอาชีวศึกษาเชียงรายอยู่ในเกณฑ์ **ระดับปานกลาง** หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงสูงมาก** ได้แก่ ข้อ 9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ โดยมีค่าระดับความเสี่ยงอยู่ที่ 25 ข้อที่มีเกณฑ์ความเสี่ยงอยู่ใน**ระดับเสี่ยงสูง** ได้แก่ ข้อ 3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร ข้อ 5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ ข้อ 6 การควบคุมการเข้ารหัสข้อมูล มีค่าระดับความเสี่ยงอยู่ที่ 20 รองลงมาคือ ข้อ 1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ข้อ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ มีค่าระดับความเสี่ยงอยู่ที่ 16 ข้อที่มีเกณฑ์ความเสี่ยงอยู่ใน**ระดับเสี่ยงปานกลาง ได้แก่** ข้อ 4 การบริหารจัดการทรัพย์สินสารสนเทศ ข้อ 11 การควบคุมดูแลผู้ให้บริการภายนอก ข้อ 12 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ มีค่าระดับความเสี่ยงอยู่ที่ 15 รองลงมาคือ ข้อ 10 การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ ข้อ 14 การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด มีค่าระดับความเสี่ยงอยู่ที่ 12

ตาราง 27 แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษา *ภาคเหนือ 2 วิทยาลัยเทคนิคกาญจนาภิเษกเชียงราย*

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
2	การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ	4	5	20	เสี่ยงสูง

ตาราง 27 (ต่อ) แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยเทคนิคกาญจนาภิเษกเชียงราย

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
3	การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร	5	5	25	เสี่ยงสูงมาก
4	การบริหารจัดการทรัพย์สินสารสนเทศ	5	5	25	เสี่ยงสูงมาก
5	การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ	4	5	20	เสี่ยงสูง
6	การควบคุมการเข้ารหัสข้อมูล	4	5	20	เสี่ยงสูง
7	การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม	5	4	20	เสี่ยงสูง
8	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ	5	4	20	เสี่ยงสูง
9	การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์	5	5	25	เสี่ยงสูงมาก
10	การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ	4	4	16	เสี่ยงสูง
11	การควบคุมดูแลผู้ให้บริการภายนอก	4	4	16	เสี่ยงสูง
12	การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	4	5	20	เสี่ยงสูง

ตาราง 27 (ต่อ) แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยเทคนิคกาญจนาภิเษกเชียงราย

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
13	การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	5	4	20	เสี่ยงสูง
14	การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด	4	4	16	เสี่ยงสูง
	รวม			**20**	**เสี่ยงสูง**

จากตาราง 27 แสดงผลการประเมินระดับความเสี่ยง ของกลุ่มตัวอย่างประเภทเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร วิทยาลัยเทคนิคกาญจนาภิเษกเชียงราย สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 พบว่า ระดับความเสี่ยงของวิทยาลัย อยู่ในเกณฑ์ **ระดับเสี่ยงสูง** หัวข้อที่อยู่ในเกณฑ์ระดับ **ระดับเสี่ยงสูงมาก** ได้แก่ ข้อ 1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบ ข้อ 3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร ข้อ 4 การบริหารจัดการทรัพย์สินสารสนเทศสารสนเทศ ข้อ 9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ มีค่าระดับความเสี่ยงอยู่ที่ 25 ข้อที่มีเกณฑ์ความเสี่ยงอยู่ใน **ระดับเสี่ยงสูง** ได้แก่ ข้อ 5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ ข้อ 6 การควบคุมการเข้ารหัสข้อมูล ข้อ 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ข้อ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ ค่าระดับความเสี่ยงอยู่ที่ 20 รองลงมา คือ ข้อ 10 การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ ข้อ 11 การควบคุมดูแลผู้ให้บริการภายนอก และข้อ 16 การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด ค่าระดับความเสี่ยงอยู่ที่ 16

ตาราง 28 แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยเทคนิคพะเยา

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
2	การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
3	การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร	5	5	25	เสี่ยงสูงมาก
4	การบริหารจัดการทรัพย์สินสารสนเทศ	5	5	25	เสี่ยงสูงมาก
5	การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ	4	5	20	เสี่ยงสูง
6	การควบคุมการเข้ารหัสข้อมูล	5	5	25	เสี่ยงสูงมาก
7	การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม	4	5	20	เสี่ยงสูง
8	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ	5	4	20	เสี่ยงสูง
9	การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์	5	5	25	เสี่ยงสูงมาก
10	การจัดหา พัฒนาและดูแลรักษา	5	4	20	เสี่ยงสูง

ระบบสารสนเทศ

ตาราง 28 (ต่อ) แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยเทคนิคพะเยา

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
11	การควบคุมดูแลผู้ให้บริการภายนอก	4	5	20	เสี่ยงสูง
12	การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	4	5	20	เสี่ยงสูง
13	การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	5	4	20	เสี่ยงสูง
14	การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด	5	4	20	เสี่ยงสูง
	รวม			21	เสี่ยงสูงมาก

จากตาราง 28 แสดงผลการประเมินระดับความเสี่ยง ของกลุ่มตัวอย่างประเภทเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร วิทยาลัยเทคนิคพะเยา สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 พบว่า ระดับความเสี่ยงของวิทยาลัย อยู่ในเกณฑ์ **ระดับเสี่ยงสูงมาก** หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงสูงมาก** ได้แก่ ข้อ 1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร ข้อ 4 การบริหารจัดการทรัพย์สินสารสนเทศ ข้อ 6 ข้อ 9 ค่าระดับความเสี่ยงอยู่ที่ 25 หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงสูง** ได้แก่ ข้อ 5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ ข้อ 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

ข้อ 10 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ ข้อ 11 การจัดหาพัฒนาและดูแลรักษาระบบสารสนเทศ ข้อ 12 การควบคุมดูแลผู้ให้บริการภายนอก ข้อ 13 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 14 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ค่าระดับความเสี่ยงอยู่ที่ 20

ตาราง 29 แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยเกษตรและเทคโนโลยีพะเยา

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
2	การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
3	การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร	5	5	25	เสี่ยงสูงมาก
4	การบริหารจัดการทรัพย์สินสารสนเทศ	5	5	25	เสี่ยงสูงมาก
5	การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ	4	5	20	เสี่ยงสูง
6	การควบคุมการเข้ารหัสข้อมูล	4	5	20	เสี่ยงสูง
7	การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม	4	4	16	เสี่ยงสูง
8	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับ	5	4	20	เสี่ยงสูง

ระบบสารสนเทศ

ตาราง 29 (ต่อ) แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยเกษตรและเทคโนโลยีพะเยา

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
9	การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์	5	5	25	เสี่ยงสูงมาก
10	การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ	4	4	16	เสี่ยงสูง
11	การควบคุมดูแลผู้ให้บริการภายนอก	4	5	20	เสี่ยงสูง
12	การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	4	5	20	เสี่ยงสูง
13	การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	5	4	20	เสี่ยงสูง
14	การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด	5	4	20	เสี่ยงสูง
	รวม			**20**	**เสี่ยงสูง**

จากตาราง 29 แสดงผลการประเมินระดับความเสี่ยง ของกลุ่มตัวอย่างประเภทเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร วิทยาลัยเกษตรและเทคโนโลยีพะเยา สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 พบว่า ระดับความเสี่ยงของวิทยาลัย อยู่ในเกณฑ์ **ระดับเสี่ยงสูง** หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงสูงมาก** ได้แก่ ข้อ 1 นโยบายด้านการรักษา

ความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร ข้อ 4 การบริหารจัดการทรัพย์สินสารสนเทศ ข้อ 9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ โดยมีค่าระดับความเสี่ยงอยู่ที่ 25 ข้อที่อยู่ในเกณฑ์**ระดับเสี่ยงสูง** ได้แก่ ข้อ 5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ ข้อ 6 การควบคุมการเข้ารหัสข้อมูล ข้อ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบการสนเทศ ข้อ 11 การควบคุมดูแลผู้ให้บริการภายนอก ข้อ 12 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 13 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 14 การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด โดยมีค่าระดับความเสี่ยงอยู่ที่ 20 รองลงมา คือ ข้อ 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ข้อ 10 การจัดหาพัฒนาและแลtรักษาระบบสารสนเทศ โดยมีค่าระดับความเสี่ยงอยู่ที่ 16

ตาราง 30 แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยเทคนิคแพร่

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
2	การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
3	การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร	3	5	15	ปานกลาง
4	การบริหารจัดการทรัพย์สินสารสนเทศ	3	4	12	ปานกลาง
5	การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ	3	5	15	ปานกลาง

6	การควบคุมการเข้ารหัสข้อมูล	4	5	20	เสี่ยงสูง

ตาราง 30 (ต่อ) แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยเทคนิคแพร่

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
7	การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม	3	4	12	ปานกลาง
8	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ	3	4	12	ปานกลาง
9	การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์	2	5	10	เสี่ยงต่ำ
10	การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ	3	4	12	ปานกลาง
11	การควบคุมดูแลผู้ให้บริการภายนอก	3	5	15	ปานกลาง
12	การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	4	4	16	เสี่ยงสูง
13	การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	3	3	9	เสี่ยงต่ำ
14	การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด	4	4	16	เสี่ยงสูง
	รวม			**15**	**ปานกลาง**

จากตาราง 30 แสดงผลการประเมินระดับความเสี่ยง ของกลุ่มตัวอย่างประเภทเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร วิทยาลัยเทคนิคแพร่สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 พบว่า ระดับความเสี่ยงของวิทยาลัย อยู่ในเกณฑ์ **ระดับเสี่ยงปานกลาง** หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงสูงมาก** ได้แก่ ข้อ 1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ โดยมีค่าระดับความเสี่ยงอยู่ที่ 25 หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงสูง** ได้แก่ ข้อ 6 การควบคุมการเข้ารหัสข้อมูล มีค่าระดับความเสี่ยงอยู่ที่ 20 ข้อ 14 การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด ข้อ 12 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ มีค่าระดับความเสี่ยงอยู่ที่ 16 หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงปานกลาง** ได้แก่ ข้อ 3 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ ข้อ 11 การควบคุมดูแลผู้ให้บริการภายนอก มีค่าระดับความเสี่ยงอยู่ที่ 15 รองลงมา คือ ข้อ 4 การบริหารจัดการทรัพย์สินสารสนเทศ ข้อ 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ข้อ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ ข้อ 10 การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศมีค่าระดับความเสี่ยงอยู่ที่ 12 หัวข้อที่อยู่ในเกณฑ์ระดับ **ระดับเสี่ยงต่ำ** ได้แก่ ข้อ 9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ มีค่าระดับความเสี่ยงอยู่ที่ 10

ตาราง 31 แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยอาชีวศึกษาแพร่

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก

2	การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ	4	4	16	เสี่ยงสูง

ตาราง 31 (ต่อ) แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยอาชีวศึกษาแพร่

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
3	การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร	3	5	15	ปานกลาง
4	การบริหารจัดการทรัพย์สินสารสนเทศ	3	4	12	ปานกลาง
5	การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ	3	5	15	ปานกลาง
6	การควบคุมการเข้ารหัสข้อมูล	4	5	20	เสี่ยงสูง
7	การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม	3	4	12	ปานกลาง
8	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ	4	4	16	ปานกลาง
9	การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์	2	5	10	เสี่ยงต่ำ
10	การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ	3	4	12	ปานกลาง
11	การควบคุมดูแลผู้ให้บริการภายนอก	3	5	15	ปานกลาง

12	การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	4	4	16	เสี่ยงสูง

ตาราง 31 (ต่อ) แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยอาชีวศึกษาแพร่

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
13	การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	4	4	16	เสี่ยงสูง
14	การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด	3	4	12	ปานกลาง
	รวม			**15**	**ปานกลาง**

จากตาราง 31 แสดงผลการประเมินระดับความเสี่ยง ของกลุ่มตัวอย่างประเภทเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร วิทยาลัยอาชีวศึกษาแพร่ สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 พบว่า ระดับความเสี่ยงของวิทยาลัย อยู่ในเกณฑ์ **ระดับเสี่ยงปานกลาง** หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงสูงมาก** ได้แก่ ข้อ 1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยมีค่าระดับความเสี่ยงอยู่ที่ 25 หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงสูง** ได้แก่ ข้อ 6 มีค่าระดับความเสี่ยงอยู่ที่ 20 หัวข้อที่อยู่ในเกณฑ์ระดับรองลงมา คือ ข้อ 2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ ข้อ 12 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 13 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ มีค่าระดับความเสี่ยงอยู่ที่ 16 หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงปานกลาง** ได้แก่ ข้อ 3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากรข้อ 5 การควบคุม

การเข้าถึงข้อมูลและระบบสารสนเทศ ข้อ 11 การควบคุมดูแลผู้ให้บริการภายนอก มีค่าระดับความเสี่ยงอยู่ที่ 15 รองลงมา คือ ข้อ 4 การบริหารจัดการทรัพย์สินสารสนเทศ ข้อ 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ข้อ 10 การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ ข้อ 14 การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด มีค่าระดับความเสี่ยงอยู่ที่ 12 หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงต่ำ** ได้แก่ ข้อ 6 การควบคุมการเข้ารหัสข้อมูล มีค่าระดับความเสี่ยงอยู่ที่ 10

ตาราง 32 แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยเกษตรและเทคโนโลยีแพร่

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
2	การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
3	การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร	5	5	25	เสี่ยงสูงมาก
4	การบริหารจัดการทรัพย์สินสารสนเทศ	5	5	25	เสี่ยงสูงมาก
5	การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ	4	5	20	เสี่ยงสูง
6	การควบคุมการเข้ารหัสข้อมูล	4	5	20	เสี่ยงสูง
7	การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม	5	4	20	เสี่ยงสูง
8	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ	5	4	20	เสี่ยงสูง

9	การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์	5	5	25	เสี่ยงสูงมาก

ตาราง 32 (ต่อ) แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยเกษตรและเทคโนโลยีแพร่

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
10	การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ	5	4	20	เสี่ยงสูง
11	การควบคุมดูแลผู้ให้บริการภายนอก	4	5	20	เสี่ยงสูง
12	การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	4	5	20	เสี่ยงสูง
13	การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	5	4	20	เสี่ยงสูง
14	การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด	5	4	20	เสี่ยงสูง
	รวม			**21**	**เสี่ยงสูงมาก**

จากตาราง 32 แสดงผลการประเมินระดับความเสี่ยง ของกลุ่มตัวอย่างประเภทเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร วิทยาลัยเกษตรและเทคโนโลยีแพร่ สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 พบว่า ระดับความเสี่ยงของวิทยาลัยเกษตรและเทคโนโลยีแพร่ อยู่ในเกณฑ์ **ระดับเสี่ยงสูงมาก** หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงสูงมาก** ได้แก่ ข้อ 1 นโยบายด้านการรักษาความมั่นคงลอดภัยของระบบสารสนเทศ ข้อ 2 การจัดโครงสร้าง

ความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร ข้อ 4 การบริหารจัดการทรัพย์สินสารสนเทศ ข้อ 9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ โดยมีค่าระดับความเสี่ยงอยู่ที่ 25 หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงสูง** ได้แก่ ข้อ 5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ ข้อ 6 การควบคุมการเข้ารหัสข้อมูล ข้อ 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ข้อ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ ข้อ 10 การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ ข้อ 11 การควบคุมดูแลผู้ให้บริการภายนอก ข้อ 12 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 13 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 14 การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด โดยมีค่าระดับความเสี่ยงอยู่ที่ 20

ตาราง 33 แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยเทคนิคน่าน

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
1	นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
2	การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ	5	5	25	เสี่ยงสูงมาก
3	การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร	5	5	25	เสี่ยงสูงมาก
4	การบริหารจัดการทรัพย์สินสารสนเทศ	5	5	25	เสี่ยงสูงมาก
5	การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ	4	5	20	เสี่ยงสูง
6	การควบคุมการเข้ารหัสข้อมูล	4	5	20	เสี่ยงสูง

7	การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม	5	4	20	เสี่ยงสูง

ตาราง 33 (ต่อ) แสดงผลภาพรวมการประเมินระดับความเสี่ยง ของกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 วิทยาลัยเทคนิคน่าน

ด้าน	คำถาม	โอกาส	ผลกระทบ	ค่าความเสี่ยง	ระดับความเสี่ยง
8	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ	4	4	16	เสี่ยงสูง
9	การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์	5	5	25	เสี่ยงสูงมาก
10	การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ	5	4	20	เสี่ยงสูง
11	การควบคุมดูแลผู้ให้บริการภายนอก	4	5	20	เสี่ยงสูง
12	การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	4	5	20	เสี่ยงสูง
13	การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	5	4	20	เสี่ยงสูง
14	การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด	5	4	20	เสี่ยงสูง
	รวม			**20**	**เสี่ยงสูง**

จากตาราง 33 แสดงผลการประเมินระดับความเสี่ยง ของกลุ่มตัวอย่างประเภทเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร วิทยาลัยเทคนิคน่าน สถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ 2 พบว่า ระดับความเสี่ยงของวิทยาลัยเทคนิคน่าน อยู่ในเกณฑ์ **ระดับเสี่ยงสูง** หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงสูงมาก** ได้แก่ ข้อ 1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร ข้อ 4 การบริหารจัดการทรัพย์สินสารสนเทศ ข้อ 9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ โดยมีค่าระดับความเสี่ยงอยู่ที่ 25 หัวข้อที่อยู่ในเกณฑ์ **ระดับเสี่ยงสูง** ได้แก่ ข้อ 5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ ข้อ 6 การควบคุมการเข้ารหัสข้อมูล ข้อ 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ข้อ 10 การจัดหาพัฒนาและดูแลรักษาระบบสารสนเทศ ข้อ 11 การควบคุมดูแลผู้ให้บริการภายนอก ข้อ 12 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 13 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อ 14 การควบคุมกระบวนการทำงาน ให้เป็นไปตามข้อกำหนด มีค่าระดับความเสี่ยงอยู่ที่ 20 รองลงมา คือ ข้อ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ มีค่าระดับความเสี่ยงอยู่ที่ 16

4. ผลการประเมินความพึงพอใจการใช้งานระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร (ITRSM) ขององค์กรในภาพรวม

ตอนที่ 1 ผลการวิเคราะห์ข้อมูลทั่วไปของกลุ่มผู้ใช้งานระบบ (ITRSM)

ตอนที่ 2 ผลการวิเคราะห์ระดับความพึงพอใจการใช้บริการระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร (ITRSM)

ส่วนที่ 1 ผลการวิเคราะห์ข้อมูลทั่วไปของประชากรกลุ่มตัวอย่าง

ตาราง 34 แสดงข้อมูลทั่วไปของผู้ตอบคำถามระดับความพึงพอใจการใช้งานระบบ *ITRSM*

ลักษณะทางประชากร	จำนวน (คน)	ร้อยละ

1. เพศ		
–ชาย	1	10
–หญิง	10	90
2. ระดับการศึกษา		
ปริญญาตรี	11	100

ตาราง 34 (ต่อ) แสดงข้อมูลทั่วไปของผู้ตอบคำถามระดับความพึงพอใจการใช้งานระบบITRSM

ลักษณะทางประชากร	จำนวน (คน)	ร้อยละ
3. ประเภทผู้ใช้งานระบบ		
–ผู้ใช้งานทั่วไป	10	90
–เจ้าหน้าที่ผู้ดูแลระบบ	1	10

จากตาราง 34 แสดงลักษณะประชากร กลุ่มผู้ใช้งานระบบ (ITRSM) สถาบันการอาชีวศึกษาภาคเหนือ 2 จำแนกลักษณะประชากรได้ ดังนี้

เพศ กลุ่มตัวอย่างทั้งหมดเป็นเพศชาย จำนวน 1 คน คิดเป็นร้อยละ 10 และเพศหญิง จำนวน 10 คน คิดเป็นร้อยละ 90

ระดับการศึกษา กลุ่มตัวอย่างมีระดับการศึกษา ระดับปริญญาตรี จำนวน 11 คน คิดเป็นร้อยละ 100

ประเภทผู้ใช้งานระบบ กลุ่มตัวอย่างการศึกษา เป็นกลุ่มประเภทผู้ใช้งานทั่วไป จำนวน 10 คน คิดเป็นร้อยละ 90 และเจ้าหน้าที่ผู้ดูแลระบบ จำนวน 1 คน คิดเป็นร้อยละ 10

ตาราง 35 แสดงด้านที่ 1 เนื้อหา

ข้อ	รายการ	ระดับความพึงพอใจ			
		ร้อยละ	ค่าเฉลี่ย	SD	แปรผล
1	ข้อมูลมีประโยชน์เนื้อหาครอบคลุมตามหลักการใช้งาน	80	4.00	0.60	มาก
2	ประโยชน์ในการนำไปปรับใช้ในการทำงาน	88	4.27	0.62	มาก
3	ความสะดวกในการเรียกดูและสืบค้นข้อมูล	42	2.18	0.83	น้อย
4	การเข้าถึงระบบทำได้ง่ายและรวดเร็ว	52	2.73	0.62	ปานกลาง
5	เมนูการใช้งานง่าย	76	3.73	0.96	มาก

6	รายงานผลได้ตามต้องการสามารถนำไปใช้ตัดสินใจได้	70	3.45	0.50	ปานกลาง
7	ความถูกต้อง ชัดเจน น่าเชื่อถือของข้อมูล	88	4.27	0.62	มาก
8	ปริมาณข้อมูลในแบบทดสอบ	80	4.00	0.74	มาก
	รวม	**72**	**3.58**	**0.69**	**มาก**

จากตาราง 35 แสดงด้านที่ 1 เนื้อหา มีรายการทั้งหมด 8 รายการ กลุ่มผู้ใช้งานระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศขององค์กรในภาพรวม มีความพึงพอใจด้านเนื้อหา อยู่ใน **ระดับมาก** มีค่าเฉลี่ยอยู่ที่ 3.58 ซึ่งหากพิจารณาเป็นรายข้อ พบว่า ระดับความพึงพอใจอยู่ใน **ระดับมาก** ได้แก่ ประโยชน์ในการนำไปปรับใช้ในการทำงาน มีค่าเฉลี่ยอยู่ที่ 4.27 ความถูกต้อง ชัดเจน น่าเชื่อถือของข้อมูล มีค่าเฉลี่ยอยู่ที่ 4.27 ข้อมูลมีประโยชน์เนื้อหาครอบคลุมตามหลักการใช้งาน มีค่าเฉลี่ยอยู่ที่ 4.00 ปริมาณข้อมูลในแบบทดสอบ มีค่าเฉลี่ยอยู่ที่ 4.00 เมนูการใช้งานง่าย มีค่าเฉลี่ยอยู่ที่ 3.73 รองลงมามีความพึงพอใจ อยู่ใน **ระดับปานกลาง** ได้แก่ รายงานผลได้ตามต้องการสามารถนำไปใช้ตัดสินใจได้ มีค่าเฉลี่ยอยู่ที่ 3.45 การเข้าถึงระบบทำได้ง่ายและรวดเร็ว มีค่าเฉลี่ยอยู่ที่ 2.73 สำหรับความพึงพอใจอยู่ใน**ระดับน้อย** ได้แก่ ความสะดวกในการเรียกดูและสืบค้นข้อมูล มีค่าเฉลี่ยอยู่ที่ 2.18

ตาราง 36 แสดงด้านที่ 2 การออกแบบ

ข้อ	รายการ	ระดับความพึงพอใจ			
		ร้อยละ	ค่าเฉลี่ย	SD	แปรผล
9	ความสวยงามและน่าสนใจของระบบ	53	2.64	0.48	ปานกลาง
10	การจัดรูปแบบง่ายต่อการใช้งาน	55	2.73	0.45	ปานกลาง
11	ความเร็วในการแสดงผลข้อมูล	49	2.45	0.66	น้อย
12	ข้อความสื่อความหมายชัดเจน	56	2.82	0.57	ปานกลาง
13	ความเหมาะสมของรูปแบบการรายงาน	35	1.73	0.45	น้อย
	รวม	**49**	**2.47**	**0.52**	**น้อย**

จากตาราง 36 ด้านที่ 2 การออกแบบ มีรายการทั้งหมด 5 รายการ กลุ่มผู้ใช้งานระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศขององค์กรในภาพรวม มีความพึงพอใจ

ด้านการออกแบบอยู่ใน **ระดับน้อย** มีค่าเฉลี่ยอยู่ที่ 2.47 ซึ่งหากพิจารณาเป็นรายข้อ พบว่า ระดับความพึงพอใจอยู่ใน **ระดับปานกลาง** ได้แก่ ข้อความสื่อความหมายชัดเจน มีค่าเฉลี่ยอยู่ที่ 2.82 การจัดรูปแบบง่ายต่อการใช้งาน มีค่าเฉลี่ยอยู่ที่ 2.73 และความสวยงามและน่าสนใจของระบบ มีค่าเฉลี่ยอยู่ที่ 2.64 รองลงมา คือ ความพึงพอใจอยู่ใน **ระดับน้อย** ได้แก่ ความเร็วในการแสดงผลข้อมูล มีค่าเฉลี่ยอยู่ที่ 2.45 และความเหมาะสมของรูปแบบการรายงาน มีค่าเฉลี่ยอยู่ที่ 1.73

ตาราง 37 แสดงด้านที่ 3 การใช้งานระบบ

ข้อ	รายการ	ระดับความพึงพอใจ			
		ร้อยละ	ค่าเฉลี่ย	SD	แปรผล
14	ระบบใช้งานง่าย มีความสะดวกในการทำทดสอบเมนูไม่ซับซ้อน	55	2.73	0.45	ปานกลาง
15	ความชัดเจนของคำอธิบาย ส่วนประกอบต่าง ๆ บนหน้าจอของระบบ	56	2.82	0.57	ปานกลาง
16	ระบบมีการประมวลผลที่รวดเร็วแม่นยำและถูกต้อง	55	2.73	0.45	ปานกลาง
17	ระบบมีการแจ้งเตือนการทำงาน เมื่อมีการกรอกข้อมูลซ้ำซ้อนและการกรอกข้อมูลผิดพลาด	49	2.45	0.78	น้อย
18	ระบบสามารถช่วยลดขั้นตอนในการทำงาน	55	2.73	0.62	ปานกลาง
19	ระบบมีความพร้อมในการให้บริการแก่ผู้ใช้อยู่เสมอ	51	2.55	0.89	ปานกลาง
20	ระบบมีความเป็นปัจจุบันของข้อมูล	58	2.91	0.79	ปานกลาง
	รวม	**54**	**2.70**	**0.65**	**ปานกลาง**

จากตาราง 37 แสดงด้านที่ 3 การใช้งานระบบ มีรายการทั้งหมด 7 รายการ กลุ่มผู้ใช้งานระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศขององค์กรในภาพรวม มีความพึงพอใจด้านการใช้งานระบบอยู่ใน **ระดับปานกลาง** มีค่าเฉลี่ยอยู่ที่ 2.71 ซึ่งหากพิจารณาเป็นรายข้อ พบว่า ระดับความพึงพอใจอยู่ใน **ระดับปานกลาง** ได้แก่ ระบบมีความ

เป็นปัจจุบันของข้อมูล 2.91 ความชัดเจนของคำอธิบาย ส่วนประกอบต่าง ๆ บนหน้าจอของระบบมีค่าเฉลี่ยอยู่ที่ 2.82 ระบบใช้งานง่าย มีความสะดวกในการทำทดสอบเมนูไม่ซับซ้อน มีค่าเฉลี่ยอยู่ที่ 2.73 ระบบมีการประมวลผลที่รวดเร็ว แม่นยำและถูกต้อง มีค่าเฉลี่ยอยู่ที่ 2.73 ระบบสามารถช่วยลดขั้นตอนในการทำงาน 2.73 และระบบมีความพร้อมในการให้บริการแก่ผู้ใช้อยู่เสมอ มีค่าเฉลี่ยอยู่ที่ 2.55 สำหรับความพึงพอใจอยู่ใน **ระดับน้อย** ได้แก่ ระบบมีการแจ้งเตือนการทำงาน เมื่อมีการกรอกข้อมูลซ้ำซ้อนและการกรอกข้อมูลผิดพลาด มีค่าเฉลี่ยอยู่ที่ 2.45

ตาราง 38 แสดงด้านที่ 4 คุณภาพระบบ

ข้อ	รายการ	ระดับความพึงพอใจ			
		ร้อยละ	ค่าเฉลี่ย	SD	แปรผล
21	ความพึงพอใจในการใช้งานของระบบในภาพรวม	55	2.73	0.75	ปานกลาง
22	ความสามารถของระบบในการนำไปปรับใช้งาน	47	2.36	0.48	น้อย
	รวม	**51**	**2.55**	**0.62**	ปานกลาง

จากตาราง 38 แสดงด้านที่ 4 คุณภาพระบบ มีรายการทั้งหมด 2 รายการ กลุ่มผู้ใช้งานระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศขององค์กรในภาพรวม มีความพึงพอใจด้านคุณภาพระบบอยู่ใน **ระดับปานกลาง** มีค่าเฉลี่ยอยู่ที่ 2.55 ซึ่งหากพิจารณาเป็นรายข้อ พบว่า ระดับความพึงพอใจอยู่ใน **ระดับปานกลาง** ได้แก่ ความพึงพอใจในการใช้งานของระบบในภาพรวมมีค่าเฉลี่ยอยู่ที่ 2.73 รองลงมา คือ ความพึงพอใจอยู่ใน**ระดับน้อย** ได้แก่ ความสามารถของระบบในการนำไปปรับใช้งานระบบ มีค่าเฉลี่ยอยู่ที่ 2.36

5. ผลการประเมินความพึงพอใจการใช้งานระบบประเมินความเสี่ยงเทคโนโลยีสารสนเทศในองค์กร (ITRSM) ของกลุ่มตัวอย่าง

กลุ่มผู้ใช้งานทั่วไป

ตอนที่ 1 ผลการวิเคราะห์ข้อมูลทั่วไปของกลุ่มผู้ใช้งานระบบ (ITRSM)

ตอนที่ 2 ผลการวิเคราะห์ระดับความพึงพอใจการใช้บริการระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร (ITRSM)

ส่วนที่ 1 ผลการวิเคราะห์ข้อมูลทั่วไปของประชากรกลุ่มตัวอย่าง

ตาราง 39 แสดงข้อมูลทั่วไปของผู้ตอบคำถามระดับความพึงพอใจการใช้งานระบบ

ลักษณะทางประชากร	จำนวน (คน)	ร้อยละ
1. เพศ		
หญิง	10	100
2. ระดับการศึกษา		
ปริญญาตรี	10	100
3. ประเภทผู้ใช้งานระบบ		
ผู้ใช้งานทั่วไป	10	100

จากตาราง 39 แสดงลักษณะประชากร กลุ่มผู้ใช้งานทั่ว สถานบันการอาชีวศึกษาภาคเหนือ 2 จำแนกลักษณะประชากรได้ ดังนี้

เพศ กลุ่มตัวอย่างทั้งหมดเป็นเพศหญิง จำนวน 10 คน คิดเป็นร้อยละ 100

ระดับการศึกษา กลุ่มตัวอย่างมีระดับการศึกษา ระดับปริญญาตรี จำนวน 10 คน คิดเป็นร้อยละ 100

ประเภทผู้ใช้งานระบบ กลุ่มตัวอย่างการศึกษา เป็นกลุ่มประเภทผู้ใช้งานทั่วไป จำนวน 10 คน คิดเป็นร้อยละ 100

ตาราง 40 แสดงด้านที่ 1 เนื้อหา

ข้อ	รายการ	ระดับความพึงพอใจ			
		ร้อยละ	ค่าเฉลี่ย	SD	แปรผล

1	ข้อมูลมีประโยชน์เนื้อหาครอบคลุมตามหลักการใช้งาน	80	4.00	0.63	มาก
2	ประโยชน์ในการนำไปปรับใช้ในการทำงาน	88	4.40	0.49	มาก
3	ความสะดวกในการเรียกดูและสืบค้นข้อมูล	42	2.10	0.83	น้อย
4	การเข้าถึงระบบทำได้ง่ายและรวดเร็ว	52	2.60	0.49	ปานกลาง
5	เมนูการใช้งานง่าย	76	3.80	1.00	มาก

ตาราง 41 (ต่อ) แสดงด้านที่ 1 เนื้อหา

ข้อ	รายการ	ระดับความพึงพอใจ			
		ร้อยละ	ค่าเฉลี่ย	SD	แปรผล
6	รายงานผลได้ตามต้องการสามารถนำไปใช้ตัดสินใจได้	70	3.50	0.50	ปานกลาง
7	ความถูกต้อง ชัดเจน น่าเชื่อถือของข้อมูล	88	4.40	0.49	มาก
8	ปริมาณข้อมูลในแบบทดสอบ	80	4.00	0.77	ปานกลาง
	รวม	**72.27**	**3.61**	**0.65**	**มาก**

จากตาราง 40 แสดงด้านที่ 1 เนื้อหา มีรายการทั้งหมด 8 รายการ กลุ่มผู้ใช้งานระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร ประเภท เจ้าหน้าที่ทั่วไป มีความพึงพอใจด้านเนื้อหาในภาพรวม อยู่ในระดับ มาก มีค่าเฉลี่ยอยู่ที่ 3.61 ซึ่งหากพิจารณาเป็นรายข้อ พบว่า ระดับความพึงพอใจอยู่ใน **ระดับมาก** ได้แก่ ประโยชน์ในการนำไปปรับใช้ในการทำงาน มีค่าเฉลี่ยอยู่ที่ 4.40 ความถูกต้องชัดเจน น่าเชื่อถือของข้อมูล มีค่าเฉลี่ยอยู่ที่ 4.40 ข้อมูลมีประโยชน์เนื้อหาครอบคลุมตามหลักการใช้งานมีค่าเฉลี่ยมีค่าเฉลี่ยอยู่ที่ 4.40 ปริมาณข้อมูลในแบบทดสอบ มีค่าเฉลี่ยอยู่ที่ 4.00 เมนูการใช้งานง่ายมีค่าเฉลี่ยอยู่ที่ 3.91 รองลงมามีความพึงพอใจ อยู่ใน **ระดับปานกลาง** ได้แก่ รายงานผลได้ตามต้องการสามารถนำไปใช้ตัดสินใจได้ มีค่าเฉลี่ย 3.50 การเข้าถึงระบบทำได้ง่ายและรวดเร็ว มีค่าเฉลี่ยอยู่ที่ 2.60 สำหรับความพึงพอใจอยู่ในระดับน้อย ได้แก่ ความสะดวกในการเรียกดูและสืบค้นข้อมูล มีค่าเฉลี่ยอยู่ที่ 2.10

ตาราง 42 แสดงด้านที่ 2 การออกแบบ

ข้อ	รายการ	ระดับความพึงพอใจ			
		ร้อยละ	ค่าเฉลี่ย	SD	แปรผล
9	ความสวยงามและน่าสนใจของระบบ	52	2.60	0.49	ปานกลาง
10	การจัดรูปแบบง่ายต่อการใช้งาน	54	2.70	0.46	ปานกลาง
11	ความเร็วในการแสดงผลข้อมูล	48	2.40	0.66	น้อย
12	ข้อความสื่อความหมายชัดเจน	54	2.70	0.64	มาก
13	ความเหมาะสมของรูปแบบการรายงาน	34	1.70	0.46	น้อย
	รวม	**48**	**2.42**	**0.51**	**น้อย**

จากตาราง 41 แสดงด้านที่ 2 การออกแบบ มีรายการทั้งหมด 5 รายการ กลุ่มผู้ใช้งานระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร ประเภท เจ้าหน้าที่ทั่วไป ความพึงพอใจด้านการออกแบบในภาพรวมอยู่ใน **ระดับน้อย** มีค่าเฉลี่ยอยู่ที่ 2.44 ซึ่งหากพิจารณาเป็นรายข้อพบว่า ระดับความพึงพอใจอยู่ใน **ระดับมาก** ได้แก่ ข้อความสื่อความหมายชัดเจน มีค่าเฉลี่ยอยู่ที่ 2.70 รองลงมา คือ ความพึงพอใจอยู่ใน **ระดับปานกลาง** ได้แก่ การจัดรูปแบบง่ายต่อการใช้งาน มีค่าเฉลี่ยอยู่ที่ 2.70 และความสวยงามและน่าสนใจของระบบ มีค่าเฉลี่ยอยู่ที่ 2.60 สำหรับความพึงพอใจอยู่ในระดับน้อย ได้แก่ ความเร็วในการแสดงผลข้อมูล มีค่าเฉลี่ย 2.40 และความเหมาะสมของรูปแบบการรายงานมีค่าเฉลี่ยอยู่ที่ 1.70

ตาราง 43 แสดงด้านที่ 3 การใช้งานระบบ

ข้อ	รายการ	ระดับความพึงพอใจ			
		ร้อยละ	ค่าเฉลี่ย	SD	แปรผล
14	ระบบใช้งานง่าย มีความสะดวกในการทำทดสอบเมนูไม่ซับซ้อน	54	2.70	0.46	ปานกลาง
15	ความชัดเจนของคำอธิบาย ส่วนประกอบต่าง ๆ บนหน้าจอของระบบ	54	2.70	0.46	ปานกลาง
16	ระบบมีการประมวลผลที่รวดเร็ว แม่นยำและถูกต้อง	54	2.70	0.46	ปานกลาง
17	ระบบมีการแจ้งเตือนการทำงานเมื่อมีการกรอกข้อมูลซ้ำซ้อนและ	50	2.50	0.81	น้อย

	การกรอกข้อมูลผิดพลาด				
18	ระบบสามารถช่วยลดขั้นตอนในการทำงาน	54	2.70	0.46	ปานกลาง
19	ระบบมีความพร้อมในการให้บริการแก่ผู้ใช้อยู่เสมอ	52	2.60	0.92	ปานกลาง
20	ระบบมีความเป็นปัจจุบันของข้อมูล	56	2.80	0.75	ปานกลาง
	รวม	**53.43**	**2.67**	**0.64**	**ปานกลาง**

จากตาราง 42 แสดงด้านที่ 3 การใช้งานระบบ มีรายการทั้งหมด 7 รายการ กลุ่มผู้ใช้งานระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร ประเภทเจ้าหน้าที่ทั่วไป มีความพึงพอใจด้านการใช้งานระบบในภาพรวมอยู่ใน **ระดับปานกลาง** มีค่าเฉลี่ยอยู่ที่ 2.64 ซึ่งหากพิจารณาเป็นรายข้อ พบว่า ระดับความพึงพอใจอยู่ใน **ระดับปานกลาง** ได้แก่ ระบบมีความเป็นปัจจุบันของข้อมูล 2.80ระบบใช้งานง่าย มีความสะดวกในการทำทดสอบเมนูไม่ซับซ้อน มีค่าเฉลี่ยอยู่ที่ 2.70 ความชัดเจนของคำอธิบายส่วนประกอบต่าง ๆ บนหน้าจอของระบบ มีค่าเฉลี่ยอยู่ที่ 2.70 ระบบมีการประมวลผลที่รวดเร็วแม่นยำและถูกต้อง มีค่าเฉลี่ยอยู่ที่ 2.70 และระบบสามารถช่วยลดขั้นตอนในการทำงาน 2.70 รองลงมา คือ ความพึงพอใจอยู่ใน**ระดับน้อย** ได้แก่ ระบบมีการแจ้งเตือนการทำงานเมื่อมีการกรอกข้อมูลซ้ำซ้อนและการกรอกข้อมูลผิดพลาด มีค่าเฉลี่ยอยู่ที่ 2.50

ตาราง 44 แสดงด้านที่ 4 คุณภาพระบบ

ข้อ	รายการ	ระดับความพึงพอใจ			
		ร้อยละ	ค่าเฉลี่ย	SD	แปรผล
21	ความพึงพอใจในการใช้งานของระบบในภาพรวม	56	2.80	0.75	ปานกลาง
22	ความสามารถของระบบในการนำไปปรับใช้งาน	46	2.30	0.46	น้อย
	รวม	**51**	**2.55**	**0.60**	**ปานกลาง**

จากตาราง 43 แสดงด้านที่ 4 คุณภาพระบบ มีรายการทั้งหมด 2 รายการ กลุ่มผู้ใช้งานระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร ประเภทเจ้าหน้าที่ทั่วไปมีความพึงพอใจด้านคุณภาพระบบในภาพรวมอยู่ใน **ระดับปานกลาง** มีค่าเฉลี่ยอยู่ที่ 2.55 ซึ่งหากพิจารณาเป็นรายข้อ พบว่า ระดับความพึงพอใจอยู่ใน **ระดับปานกลาง** ได้แก่ความพึงพอใจในการใช้งานของระบบในภาพรวม มีค่าเฉลี่ยอยู่ที่ 2.80 รองลงมา คือ ความพึงพอใจอยู่ในระดับน้อย ได้แก่ ความสามารถของระบบในการนำไปปรับใช้งานระบบ มีค่าเฉลี่ยอยู่ที่ 2.30

กลุ่มเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร

ตอนที่ 1 ผลการวิเคราะห์ข้อมูลทั่วไปของกลุ่มผู้ใช้งานระบบ (ITRSM)

ตอนที่ 2 ผลการวิเคราะห์ระดับความพึงพอใจการใช้บริการระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร (ITRSM)

ส่วนที่ 1 ผลการวิเคราะห์ข้อมูลทั่วไปของประชากรกลุ่มตัวอย่าง

ตาราง 45 แสดงข้อมูลทั่วไปของผู้ตอบคำถามระดับความพึงพอใจการใช้งานระบบ *ITRSM*

ลักษณะทางประชากร	จำนวน (คน)	ร้อยละ
1. เพศ		
ชาย	1	100
2. ระดับการศึกษา		
ปริญญาตรี	1	100
3. ประเภทผู้ใช้งานระบบ		
เจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร	1	100

ตาราง 44 แสดงลักษณะประชากร กลุ่มตัวอย่าง เจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กรสถาบันการอาชีวศึกษาภาคเหนือ 2 จำแนกลักษณะประชากรได้ ดังนี้

เพศ กลุ่มตัวอย่างทั้งหมดเป็นเพศชาย จำนวน 1 คน คิดเป็นร้อยละ 100

ระดับการศึกษา กลุ่มตัวอย่างมีระดับการศึกษา ระดับปริญญาตรี จำนวน 1 คน คิดเป็นร้อยละ 100

ประเภทผู้ใช้งานระบบ กลุ่มตัวอย่างการศึกษา เป็นกลุ่มประเภท เจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร จำนวน 1 คน คิดเป็นร้อยละ 100

ตาราง 46 แสดงด้านที่ 1 เนื้อหา

ข้อ	รายการ	ระดับความพึงพอใจ			
		ร้อยละ	ค่าเฉลี่ย	SD	แปรผล
1	ข้อมูลมีประโยชน์ เนื้อหาครอบคลุมตามหลักการใช้งาน	80	4.00	0	มาก
2	ประโยชน์ในการนำไปปรับใช้ในการทำงาน	60	3.00	0	ปานกลาง
3	ความสะดวกในการเรียกดูและสืบค้นข้อมูล	60	3.00	0	ปานกลาง
4	การเข้าถึงระบบทำได้ง่ายและรวดเร็ว	80	4.00	0	มาก
5	เมนูการใช้งานง่าย	60	3.00	0	ปานกลาง
6	รายงานผลได้ตามต้องการสามารถนำไปใช้ตัดสินใจได้	60	3.00	0	ปานกลาง
7	ความถูกต้อง ชัดเจน น่าเชื่อถือของข้อมูล	60	3.00	0	ปานกลาง
8	ปริมาณข้อมูลในแบบทดสอบ	80	4.00	0	มาก
	รวม	**68**	**3.38**	**0**	**ปานกลาง**

จากตาราง 45 แสดงด้านที่ 1 เนื้อหา มีรายการทั้งหมด 8 รายการ กลุ่มผู้ใช้งานระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร ประเภท เจ้าหน้าที่ดูแล

ระบบสารสนเทศในองค์กร มีความพึงพอใจด้านคุณภาพระบบในภาพรวมอยู่ใน **ระดับปานกลาง**มีค่าเฉลี่ยอยู่ที่ 3.38 ซึ่งหากพิจารณาเป็นรายข้อ พบว่า ระดับความพึงพอใจอยู่ใน **ระดับมาก** ได้แก่ ข้อมูลมีประโยชน์ เนื้อหาครอบคลุมตามหลักการใช้งาน มีค่าเฉลี่ยอยู่ที่ 4.00 การเข้าถึงระบบทำได้ง่ายและรวดเร็ว มีค่าเฉลี่ยอยู่ที่ 4.00 และปริมาณข้อมูลในแบบทดสอบ มีค่าเฉลี่ยอยู่ที่ 4.00 รองลงมา คือ ความพึงพอใจอยู่ใน **ระดับปานกลาง** ได้แก่ ประโยชน์ในการนำไปปรับใช้ในการทำงาน มีค่าเฉลี่ยอยู่ที่ 3.00 ความสะดวกในการเรียกดูและสืบค้นข้อมูล มีค่าเฉลี่ยอยู่ที่ 3.00 เมนูการใช้งานง่าย มีค่าเฉลี่ยอยู่ที่ 3.00 รายงานผลได้ตามต้องการ สามารถนำไปปรับใช้ตัดสินใจได้ มีค่าเฉลี่ยอยู่ที่ 3.00 และความถูกต้อง ชัดเจน น่าเชื่อถือของข้อมูล มีค่าเฉลี่ยอยู่ที่ 3.00

ตาราง 47 แสดงด้านที่ 2 การออกแบบ

ข้อ	รายการ	ระดับความพึงพอใจ			
		ร้อยละ	ค่าเฉลี่ย	SD	แปรผล
9	ความสวยงามและน่าสนใจของระบบ	60	3.00	0	ปานกลาง
10	การจัดรูปแบบง่ายต่อการใช้งาน	60	3.00	0	ปานกลาง
11	ความเร็วในการแสดงผลข้อมูล	60	3.00	0	ปานกลาง
12	ข้อความสื่อความหมายชัดเจน	80	4.00	0	มาก
13	ความเหมาะสมของรูปแบบการรายงาน	40	2.00	0	น้อย
	รวม	**60**	**3.00**	**0**	**ปานกลาง**

จากตาราง 48 แสดงด้านที่ 2 การออกแบบ มีรายการทั้งหมด 5 รายการ กลุ่มผู้ใช้งานระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร ประเภทเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กรมีความพึงพอใจด้านด้านคุณภาพระบบในภาพรวมอยู่ใน **ระดับปานกลาง** มีค่าเฉลี่ย อยู่ที่ 3.00 ซึ่งหากพิจารณาเป็นรายข้อ พบว่า ระดับความพึงพอใจอยู่ใน**ระดับมาก** ได้แก่ ข้อความสื่อความหมายชัดเจนมีค่าเฉลี่ยอยู่ที่ 4 รองลงมา คือความพึงพอใจอยู่ใน**ระดับปานกลาง** ได้แก่ ความสวยงามและน่าสนใจของระบบ มีค่าเฉลี่ยอยู่ที่ 3 การจัดรูปแบบง่ายต่อการใช้งาน มีค่าเฉลี่ยอยู่ที่ 3 สำหรับความพึงพอใจอยู่ใน **ระดับน้อย** ได้แก่ ความเหมาะสมของรูปแบบการรายงาน มีค่าเฉลี่ยอยู่ที่ 2.00

ตาราง 48 แสดงด้านที่ 3 การใช้งานระบบ

ข้อ	รายการ	ระดับความพึงพอใจ			
		ร้อยละ	ค่าเฉลี่ย	SD	แปรผล
14	ระบบใช้งานง่าย มีความสะดวกในการทำทดสอบเมนูไม่ซับซ้อน	60	3.00	0	ปานกลาง
15	ความชัดเจนของคำอธิบายส่วนประกอบต่าง ๆ บนหน้าจอของระบบ	40	2.00	0	น้อย
16	ระบบมีการประมวลผลที่รวดเร็วแม่นยำและถูกต้อง	60	3.00	0	ปานกลาง

ตาราง 49 (ต่อ) แสดงด้านที่ 3 การใช้งานระบบ

ข้อ	รายการ	ระดับความพึงพอใจ			
		ร้อยละ	ค่าเฉลี่ย	SD	แปรผล
17	ระบบมีการแจ้งเตือนการทำงานเมื่อมีการกรอกข้อมูลซ้ำซ้อนและการกรอกข้อมูลผิดพลาด	60	3.00	0	ปานกลาง
18	ระบบสามารถช่วยลดขั้นตอนในการทำงาน	60	3.00	0	ปานกลาง
19	ระบบมีความพร้อมในการให้บริการแก่ผู้ใช้อยู่เสมอ	40	2.00	0	น้อย
20	ระบบมีความเป็นปัจจุบันของข้อมูล	60	3.00	0	ปานกลาง
	รวม	**63**	**3.41**	**0**	**ปานกลาง**

จากตาราง 47 แสดงด้านที่ 3 การใช้งานระบบ มีรายการทั้งหมด 7 รายการ กลุ่มผู้ใช้งานระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร ประเภทเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร มีความพึงพอใจด้านคุณภาพระบบในภาพรวมอยู่ใน **ระดับปานกลาง** มีค่าเฉลี่ยอยู่ที่ 3.41 ซึ่งหากพิจารณาเป็นรายข้อ พบว่า ระดับความพึงพอใจอยู่ใน **ระดับมาก** ได้แก่ ความชัดเจนของคำอธิบายส่วนประกอบต่าง ๆ บนหน้าจอของระบบ มีค่าเฉลี่ยอยู่ที่ 4.00 และระบบมีความเป็นปัจจุบันของข้อมูลมีค่าเฉลี่ยอยู่ที่ 4.00 รองลงมาคือ ความพึงพอใจอยู่ใน **ระดับปานกลาง** ได้แก่ ระบบใช้งานง่าย มีความสะดวกใน

การทำทดสอบเมนูไม่ซับซ้อน มีค่าเฉลี่ยอยู่ที่ 3.00 ระบบมีการประมวลผลที่รวดเร็ว แม่นยำ และถูกต้อง มีค่าเฉลี่ยอยู่ที่ 3.00 ระบบสามารถช่วยลดขั้นตอนในการทำงาน มีค่าเฉลี่ยอยู่ที่ 3.00 สำหรับความพึงพอใจอยู่ในระดับน้อย ได้แก่ ระบบมีความพร้อมในการให้บริการแก่ผู้ใช้อยู่เสมอ

ตาราง 50 แสดงด้านที่ 4 คุณภาพระบบ

ข้อ	รายการ	ระดับความพึงพอใจ			
		ร้อยละ	ค่าเฉลี่ย	SD	แปรผล
21	ความพึงพอใจในการใช้งานของระบบในภาพรวม	40	2.00	0	น้อย
22	ความสามารถของระบบในการนำไปปรับใช้งาน	60	3.00	0	ปานกลาง
	รวม	**50.00**	**2.50**	**0**	**ปานกลาง**

จากตาราง 48 แสดงด้านที่ 4 การใช้งานระบบ มีรายการทั้งหมด 2 รายการ กลุ่มผู้ใช้งานระบบประเมินความเสี่ยงการใช้งานเทคโนโลยีสารสนเทศในองค์กร ประเภทเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร มีความพึงพอใจด้านคุณภาพระบบในภาพรวมอยู่ใน **ระดับปานกลาง** มีค่าเฉลี่ยอยู่ที่ 2.50 ซึ่งหากพิจารณาเป็นรายข้อ พบว่า ระดับความพึงพอใจอยู่ใน **ระดับปานกลาง** ได้แก่ ความสามารถของระบบในการนำไปปรับใช้งาน มีค่าเฉลี่ยอยู่ที่ 3.0 รองลงมา คือ ความพึงพอใจอยู่ใน**ระดับน้อย** ได้แก่ ความพึงพอใจในการใช้งานของระบบในภาพรวม มีค่าเฉลี่ยอยู่ที่ 2.00

บทที่ 5

บทสรุปงานวิจัย

จากการศึกษาและพัฒนาระบบประเมินความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กร ITRSM กรณีศึกษา สถาบันการอาชีวศึกษาภาคเหนือ 2 โดยการอ้างอิงมาตรฐานความปลอดภัยขั้นพื้นฐานเทคโนโลยีสารสนเทศ CIA และมาตรฐานความปลอดภัยด้านเทคโนโลยีสารสนเทศ ISO 27001 มีผลสรุปการศึกษาและข้อเสนอแนะดังต่อไปนี้

สรุปผลการวิจัย

การศึกษาค้นคว้าด้วยตนเองครั้งนี้ ได้ทำการศึกษาโดยมีวัตถุประสงค์ 1. เพื่อศึกษาและพัฒนาเครื่องมือวัดระดับความเสี่ยงการจากใช้งานเทคโนโลยีสารสนเทศในองค์กรจากการอ้างอิงมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขั้นพื้นฐาน CIA และมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ได้รับการยอมรับระดับสากล ISO 27001: 2013 2. เพื่อศึกษาระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กรของสถาบันการอาชีวศึกษาภาคเหนือ 2 และสถานศึกษาในสังกัด จำนวน 9 แห่ง

โดยผู้วิจัยได้ทำการศึกษาสภาพบริบทขององค์กรในด้านการใช้งานเทคโนโลยีสารสนเทศภายในองค์กร และศึกษาเกี่ยวกับระบบการจัดการความเสี่ยงด้านต่าง ๆ เพื่อนำมาเป็นแนวทางในการกำหนดค่าระดับความเสี่ยงในการสร้างเครื่องมือประเมินระดับความเสี่ยง ซึ่งได้ศึกษาเกี่ยวกับมาตรฐานความปลอดภัยขั้นพื้นฐานด้านเทคโนโลยีสารสนเทศ พบว่า องค์ประกอบด้านความปลอดภัยขั้นพื้นฐาน ประกอบด้วย Confidential การปกป้องสารสนเทศให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ Integrity การปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความเป็นจริง เช่น การแฮกระบบเพื่อแก้ไขข้อมูล เป็นต้น Availability การสร้างความเชื่อมั่นว่าระบบสารสนเทศมีความพร้อมใช้งานอยู่เสมอ ซึ่งองค์ประกอบต่างๆ เหล่านี้ เป็นความรู้ขั้นพื้นฐานสำหรับผู้ใช้งานทั่วไปที่มีการดำเนินงานเกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ จึงได้นำข้อมูลมากำหนดเป็นแนวทางสร้างเครื่องมือ รูปแบบคำถาม เพื่อใช้ในการวัดประเมินกับกลุ่ม เจ้าหน้าที่หรือผู้ใช้งานทั่วไปในองค์กรที่ไม่ได้มีความชำนาญหรือความรู้เฉพาะด้านเทคโนโลยีสารสนเทศ เนื่องจากในองค์กรมีกลุ่มคนที่มีองค์ความรู้และทำหน้าที่ในการดูแลรักษาระบบเทคโนโลยีสารสนเทศในองค์กร จึงได้ทำการศึกษามาตรฐานที่มีความลึกเฉพาะด้านลงไปที่เกี่ยวข้องกับลักษณะบริบทของเจ้าหน้าที่ดูแลระดับเทคโนโลยีสารสนเทศในสถาบันการอาชีวศึกษาภาคเหนือ 2

พบว่า มาตรฐาน ISO 27001:2013 ซึ่งเป็นมาตรฐานความปลอดภัยด้านเทคโนโลยีสารสนเทศที่ได้รับการยอมรับเป็นสากล

จึงได้นำเอาหัวข้อที่สำคัญ จำนวน 14 ข้อหลักมาอ้างอิง กำหนดสร้างเป็นเครื่องมือรูปแบบคำถาม กำหนดใช้กับเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กรขึ้น จากนั้นได้นำข้อคำถามทั้งสองประเภทให้ผู้เชี่ยวชาญทำการตรวจสอบความถูกต้อง เหมาะสม และได้ทำการออกแบบระบบ โดยใช้แผนภาพ Use case diagram โดยระบบประกอบด้วยผู้ใช้งาน ได้แก่ กลุ่มตัวอย่างงานวิจัย 2 ประเภท คือ กลุ่มผู้ใช้งานทั่วไปและเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร แอดมินและผู้บริหารซึ่งสามารถเข้าไปดูผลการประเมินระดับรายบุคคลและผลการประเมินรายบุคคลได้ โดยกำหนดให้ระบบทำงานได้ 3 ส่วน คือ การนำเข้าข้อมูล การประเมินผล การให้คำแนะนำ และการจัดเก็บรวบรวมผลการประเมิน ซึ่งผู้วิจัยได้ทำการออกแบบระบบการทำงานและให้ผู้มีความรู้และทักษะการเขียนโปรแกรมจัดทำระบบขึ้น โดยมีชื่อว่า ITRSM เพื่อให้ผลการประเมินนั้นยังอยู่และสามารถนำไปเป็นข้อมูลเสนอต่อผู้บริหารประกอบการตัดสินในการพัฒนาด้านเทคโนโลยีสารสนเทศในองค์กรต่อไป

หลังจากที่ได้ระบบมาแล้วผู้วิจัยได้ให้กลุ่มตัวอย่างดำเนินการทำแบบทดสอบผ่านระบบ ITRSM โดยได้มีการแบ่งหมวดการเข้าทำแบบประเมิน เป็น 2 ประเภท ได้แก่ เจ้าหน้าที่ผู้ใช้งานทั่วไปในองค์กรและเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร จากนั้น ได้ให้กลุ่มตัวอย่างร่วมประเมินความพึงพอใจการใช้งานระบบ ITRSM เพื่อเป็นแนวทางในการปรับปรุงระบบให้สามารถใช้ได้อย่างมีประสิทธิภาพต่อไป

เมื่อได้ผลการประเมินระดับความเสี่ยงฯและผลความพึงพอใจมาแล้ว ได้ส่งแบบประเมินระดับความพึงพอใจให้กับกลุ่มผู้ใช้งาน ได้แก่ กลุ่มสถานศึกษาในสังกัดสถาบันการอาชีวศึกษาภาคเหนือ จำนวน 9 แห่ง เลือกตัวแทนบุคลากรสถานศึกษาละ 10 คน เป็นตัวแทนกลุ่มเจ้าหน้าที่ทั่วไป และ 1 คน เป็นตัวแทนเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร ทำแบบทดสอบประเมินความเสี่ยงโดยไม่ผ่านระบบประเมิน เนื่องจากผลการประเมินความพึงพอใจการใช้งาน พบว่า ระบบ ยังไม่มีความพร้อมในการบันทึกผลรายองค์กรเท่าที่ควร จึงจำเป็นต้องนำผลการประเมินมาวิเคราะห์ระดับความเสี่ยงด้วยโปรแกรม Excel และแจ้งผลกลับไปยังกลุ่มผู้ใช้งานก่อน จากนั้นได้ทำการรวบรวมและสรุปผลรายสถานที่ศึกษาจัดทำเป็นข้อมูลรายงานส่งให้กับผู้บริหารสถาบันฯ ทราบต่อไป

อภิปรายผลการวิจัย

การศึกษาค้นคว้าด้วนตนเอง การประเมินความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศในองค์กร กรณี ศึกษาสถาบันการอาชีวศึกษาภาคเหนือ 2 โดยวิธีการศึกษาระดับความเสี่ยงมาตรฐานความมั่นคงปลอดภัยขั้นพื้นฐาน CIA และมาตรฐานความปลอดภัยด้านเทคโนโลยีสารสนเทศที่ได้รับการยอมรับระดับสากล ISO 27001:2013 กำหนดสร้างเครื่องมือเป็นแบบสอบถามประเมินระดับความเสี่ยงออกแบบระบบเพื่อความสะดวกในการจัดเก็บผลข้อมูลและการใช้งาน สำหรับผลการวิจัย การประเมินระดับความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กร ระดับองค์กร ของกลุ่มตัวอย่าง พบว่า สถาบันการอาชีวศึกษาภาคเหนือ 2 มีระดับความเสี่ยงด้านกลุ่มผู้ใช้งานทั่วไปอยู่ในระดับ เสี่ยงสูงมาก โดยมีจำนวนผู้ใช้งานทั่วไปในองค์กร จำนวน 10 คน เป็นผู้ทำแบบทดสอบ และผลการประเมินกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร มีจำนวน 1 คน พบ สถาบันการอาชีวศึกษาภาคเหนือ 2 มีความเสี่ยงอยู่ในระดับ เสี่ยงสูง ควรปฏิบัติตามคำแนะนำที่ได้รับอย่างเร่งด่วน

สำหรับผลจากการประเมินความพึงพอใจของผู้ใช้งานระบบ ITRSM กลุ่มตัวอย่างภาพรวมอยู่ในระดับ ปานกลาง แบ่งเป็น ความพึงพอใจด้านเนื้อหา ภาพรวมอยู่ในระดับ มาก ความพึงพอใจ ด้านการออกแบบ ภาพรวมอยู่ในระดับ น้อย ความพึงพอใจ ด้านการใช้งานของระบบ ภาพรวมอยู่ในระดับ ปานกลาง ความพึงพอใจ ด้านคุณภาพของระบบ ภาพรวมอยู่ในระดับ ปานกลาง ทั้งนี้ผลจากการประเมินความพึงพอใจการใช้งานระบบ ฯ ของกลุ่มตัวอย่างทำให้ระบบจำเป็นต้องมีการพัฒนาเพิ่มเติมอีกเพื่อให้ระบบมีประสิทธิภาพในการนำไปใช้ต่อไป

ข้อเสนอแนะ

1. ข้อเสนอแนะในการนำผลการวิจัยไปใช้

สามารถนำผลการประเมินระดับความเสี่ยงจากการใช้งานระบบเทคโนโลยีสารสนเทศในองค์กร ไปพัฒนา ปรับปรุง องค์ความรู้เกี่ยวกับการใช้งานเทคโนโลยีสารสนเทศให้มีประสิทธิภาพมากขึ้น เพื่อป้องกันความเสี่ยงอาจนำไปสู่ความเสียหายของข้อมูลในองค์กรที่อาจเกิดขึ้นได้ อีกทั้งเพื่อเป็นการนำข้อมูลในภาพรวมที่ได้ไปประกอบการตัดสินใจในการพัฒนาด้านเทคโนโลยีสารสนเทศในองค์กรต่อไป

2. ข้อเสนอแนะในการวิจัยครั้งต่อไป

งานวิจัยจำเป็นต้องมีการศึกษาลงรายละเอียดเชิงลึกของปัจจัยในแต่ละด้านให้มากกว่าเดิมและควรมีการกำหนดเนื้อหาให้สอดคล้องกับสภาพบริบทขององค์กรนั้น ๆ และ

ควรมีการอัพเดตข้อมูลอย่างสม่ำเสมอในหัวข้อด้านเนื้อหาต่าง ๆ ก่อนนำมากำหนดเป็นข้อคำถาม หากมีการทำระบบเพื่อรองรับควรมีการกำหนดขอบเขตการใช้งานให้ชัดเจนและมีความน่าสนใจมากขึ้น อีกทั้งเนื้อหาที่ใช้ในคำถามควรมีการปรับให้มีความสั้นกระชับและครอบคลุมกว่าเดิม และสามารถใช้ผลข้อมูลจากการทำแบบประเมินไปพัฒนาตัวเองในด้านการศึกษาเรียนรู้เพิ่มเติมเกี่ยวกับการใช้งานเทคโนโลยีสารสนเทศหรือการปรับประยุกต์ในการใช้ในชีวิตประจำวันได้

บรรณานุกรม

บรรณานุกรม

จิระ จิตสุภา, ปรัชญนันท์ นิลสุข, & พัลลภ พิริยะสุรวง. (2566). *ประสิทธิภาพของการฝึกอบรมออนไลน์ด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ*. Paper presented at the การประชุมวิชาการระดับชาติด้านอีเลิร์นนิง 2555, ฮอล 9 อิมแพค เมืองทองธานี.

ชนกานต์ อาภารณ์พงษ์, & บัวเรียน สูงพล. (2566). กรอบโครงร่างความมั่นคงปลอดภัยระบบสารสนเทศ (ISO 27001:2013) กรณีศึกษา สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. *วารสารดิจิทัล ธุรกิจ และสังคมศาสตร์, 9*, 1–12.

คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่. (2565). การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ. Retrieved from https://w2.Med.cmu.ac.th

จุฑามน สิทธิผลวนิชกุล. (2561). แนวทางการบริหารจัดการความเสี่ยงองค์กร COSO Enterprise Risk Management. Retrieved from WWW.Jab.tbs.tu.ac.th/files/Article/Jap42/Full/JAP42juthamon.pdf

อรวรรณ ลีลาเกียรติวณิช. (2560). *ปัจจัยที่มีผลต่อการบริหารจัดการความเสี่ยง กรณีศึกษามหาวิทยาลัยราชภัฏธนบุรี.* (บธ.ม. การศึกษาด้วยตนเอง), มหาวิทยาลัยสยาม กรุงเทพฯ.

ชุลีกร นวลสมศรี, & สุทธิศักดิ์ จันทวงษ์โส. (ม.ป.ป.). สมรรถนะด้านเทคโนโลยีสารสนเทศที่พึงประสงค์สำหรับการปฏิบัติงานของบุคลากรภาครัฐในยุคประเทศไทย 4.0. *วารสารมหาวิทยาลัยนราธิวาสราชนครินทร์, 12*, 194–206.

ณัฐนันท์ พรทวีวัฒน์, & ชัยพร เขมะภาตะพันธ์. (ม.ป.ป.). *การประเมินความเสี่ยงระบบสารสนเทศและแนวทางแก้ไข กรณีศึกษา บริษัท อาร์วีซี คอนสตั๊คชั่น จำกัด.* (วศ.ม. สารนิพนธ์), มหาวิทยาลัยธุรกิจบัณฑิตย์, กรุงเทพฯ.

บริษัท QA Hive จำกัด. (ม.ป.ป.). Retrieved from https://www.Qahive.com

บริษัท Quality Systems จำกัด. (ม.ป.ป.). Retrieved from https: //www.Qltysys.com.

พันธ์ทอง จันทร์สว่าง. (ม.ป.ป.). PT NEWs. Retrieved from https://ptsw.blogspot.com/2017/12/8-2560-eocsat-10-risk-likelihood-x.html

ล้วน สายยศ, & อังคนา สายยศ. (2538). *เทคนิคการวิจัยทางการศึกษา*. กรุงเทพฯ: ศูนย์ส่งเสริมวิชาการ.

ล้วน สายยศ, & อังคนา สายยศ. (2543). *เทคนิคการวัดผลการเรียนรู้*. กรุงเทพฯ: ศูนย์ส่งเสริมวิชาการ.

สมหทัย จารุนิมล, & นราสินธุ์ บุญมาก. องค์กรกับการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ. *วารสารมหาวิทยาลัยมหิดล, 8*, 11–25.

อรวรรณ ลีลาเกียรติวณิช. (2560). *ปัจจัยที่มีผลต่อการบริหารจัดการความเสี่ยง กรณีศึกษามหาวิทยาลัยราชภัฏธนบุรี.* (บธ.ม. การศึกษาด้วยตนเอง), มหาวิทยาลัยสยาม กรุงเทพฯ.

ภาคผนวก

ภาคผนวก ก

การสร้างเครื่องมือแบบสอบถามจากการอ้างอิงตามมาตรฐาน CIA และมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ISO 27001:2013

แบบทดสอบกลุ่มผู้ใช้งานทั่วไป

ด้าน	หัวข้ออ้างอิงจากมาตรฐาน CIA	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
1	Confidentiality: ความลับ การรักษาความลับ โดยส่วนประกอบ 2 ส่วนที่สำคัญที่จะช่วยทำให้ข้อมูลนั้นเป็นความลับได้ก็คือ การกำหนดสิทธิ์ และการพิสูจน์ตัวตน	1.1 องค์กรมีการกำหนดสิทธิ์ผู้ใช้งานเครือข่ายอินเตอร์เน็ต Log in ด้วย ID และ Password ก่อนการใช้งานทุกครั้งหรือไม่
		1.2 องค์กรมีการกำหนดกฎระเบียบเกี่ยวกับการนำอุปกรณ์ส่วนตัว มาเชื่อมต่อเครือข่ายอินเตอร์เน็ตขององค์กรหรือไม่
		1.3. อุปกรณ์คอมพิวเตอร์ที่ท่านใช้งานปัจจุบันมีการตั้งรหัสล็อคหน้าจอก่อนการเข้าใช้งานหรือไม่ หากมีท่านมีหลักการตั้งรหัสอย่างไร
		1.4. การเข้าใช้งานเว็บไซต์ต่างๆ ที่มีการ Log in ด้วย ID และ Password หรือต้องทำการยืนยันตัวตนก่อนเข้าใช้งาน ท่านมีวิธีกำหนดและจัดเก็บรหัสผ่านการเข้าใช้งานอย่างไร
		1.5. องค์กรท่านมีการกำหนดนโยบายเกี่ยวกับสิทธิในการเข้าถึงข้อมูลเทคโนโลยีสารสนเทศในองค์กรหรือไม่ ท่านปฏิบัติอย่างไรกับนโยบายดังกล่าว
		1.6. องค์กรของท่านมีการจัดทำแผนพัฒนาระบบสารสนเทศในองค์กรหรือไม่ ใครเป็นผู้ร่วมดำเนินการตามแผนดังกล่าว
		1.7 ท่านคิดว่าการจัดเก็บรหัสผ่านการเข้าใช้

ด้าน	หัวข้ออ้างอิงจากมาตรฐาน CIA	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
		งาน (E-mail) ทั้ง ID Password มีความจำเป็นหรือไม่ที่จะจัดเก็บเป็นความลับ และใครบ้างที่สามารถทราบรหัสผ่านการรเข้าใช้งานของท่านได้
2	Integrity: ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความเป็นจริง คือระบบต้องมีกลไกการตรวจสอบสิทธิหรือการได้รับอนุญาตให้ดำเนินการเปลี่ยนแปลงแก้ไขหรือกระทำการใดๆ ต่อข้อมูลนั้น	2.1 ท่านมีความขัดแย้งหรือเคยมีปัญหากับเพื่อนร่วมงานในองค์กรหรือไม่
		2.2 คุณมีวิธีการสำรองข้อมูลในงานที่รับผิดชอบอย่างไร
		2.3 ใครบ้างที่สามารถเข้าใช้งานเครื่องคอมพิวเตอร์ที่ใช้งานประจำของท่านได้
		2.4 ท่านมีการอัพเดตการใช้งานโปรแกรม Anti Virus เครื่องที่ใช้งานประจำหรือไม่ ใครเป็นผู้ดำเนินการให้
		2.5 ทุกครั้งที่เกิดปัญหาจากการใช้งานเทคโนโลยีสารสนเทศในองค์กร ท่านมีวิธีจัดการอย่างไร
		2.6 องค์กรมีการกำหนดบทลงโทษ ในกรณีที่มีการฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศและได้มีการปฏิบัติตามกฎดังกล่าวหรือไม่
3	Availability : สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน การตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิเข้าถึงระบบได้เมื่อต้องการ ภัยคุกคามต่อความพร้อมใช้งานของข้อมูล เช่น การโจมตีแบบปฏิเสธการให้บริการต้องใช้มาตรการป้องกัน เช่น การแพตช์	3.1 ระบบเครือข่ายอินเตอร์เน็ตในองค์กรของท่านสามารถเชื่อมต่อและใช้งานได้ทันทีหรือไม่
		3.2 ท่านได้มีการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ที่ใช้งานเป็นประจำสม่ำเสมอหรือไม่
		3.3 ท่านเคยได้รับการอบรมให้ความรู้เกี่ยว

ด้าน	หัวข้ออ้างอิงจากมาตรฐาน CIA	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
	ซอฟต์แวร์ปกติ การอัพเกรดระบบ การสำรองข้อมูลและการนำกลยุทธ์การกู้คืนระบบ	การใช้ระบบสารสนเทศที่ปลอดภัยภายในองค์กรหรือไม่
		3.4 ทราบหรือไม่ว่า โปรแกรมการใช้งานต่างๆบนอุปกรณ์คอมพิวเตอร์ในสำนักงานของท่าน มีที่มาจากแหล่งใด และเป็นโปรแกรมที่ถูกต้องตามลิขสิทธิ์หรือไม่
		3.5 คุณมีวิธีปฏิบัติอย่างไร เมื่อมีเหตุให้ต้องลุกออกจากการใช้งานหน้าคอมพิวเตอร์ที่กำลังใช้งานอยู่
		3.6 คุณมีหลักหรือแนวทางปฏิบัติในการในการตั้งไอดีและพาสเวิร์ดเข้าใช้งานเว็บไซต์ต่างๆอย่างไร
		3.7 ความถี่ในการเข้าเปลี่ยนรหัสการใช้งานทั้งเว็บไซค์และอุปกรณ์สารสนเทศต่างๆของคุณคือ
		3.8 ท่านกำหนดรหัสการเข้าใช้งานเว็บไซต์และอุปกรณ์ต่างๆด้วยรหัสผ่าน เดียวกันหรือไม่
		3.9 ท่านรู้จักระบบปฏิบัติการที่ใช้ในการจัดเก็บข้อมูลทางระบบออนไลน์ อย่างเช่น Cloud หรือ Google Dive หรือไม่
		3.10 เครื่องคอมพิวเตอร์ที่ท่านใช้งานเคยติดไวรัส หรือ มัลแวร์ หรือไม่
		3.11 ท่านอนุญาตให้เพื่อนร่วมงานนำแฟลชไดร์ฟมาบันทึกไฟล์งานหรือข้อมูลต่างๆยังเครื่องที่ท่านใช้งานหรือไม่
		3.12 ท่านเคยได้รับอีเมล์หรือข้อความที่ไม่ทราบแหล่งที่มาหรือไม่ และท่านปฏิบัติ

ด้าน	หัวข้ออ้างอิงจากมาตรฐาน CIA	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
		อย่างไรเมื่อได้รับอีเมลนั้น
		3.13 ท่านทราบหรือไม่ว่าไวรัสหรือมัลแวร์สามารถทำลายข้อมูลระบบและข้อมูลขององค์กรได้จากเครื่องที่ท่านใช้งานได้
		3.14 ท่านต้องการได้รับการอบรมความปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศเพิ่มเติมหรือไม่ และควรมีช่วงเวลารับการอบรมเท่าไหร่จึงจะเหมาะสมในความคิดของท่าน

ภาคผนวก ข

แบบทดสอบกลุ่มเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร

ข้อ	หัวข้อมาตรฐาน ISO 27001:2013	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
1	นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	1.1 องค์กรมีการจัดทำนโยบาย ความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษรและได้รับอนุมัติจากผู้บริหารรวมทั้งมีการสื่อสารให้บุคลากรในองค์กรรับทราบหรือไม่
		1.2 นโยบายความมั่นคงปลอดภัยสารสนเทศมีเนื้อหาที่เหมาะสม ครบถ้วนเพียงพอ และได้รับการทบทวนตามรอบระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงหรือไม่
2	การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ	2.1 องค์กรมีการกำหนดขอบเขตและมอบหมายหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศให้แก่พนักงานภายในองค์กร คู่สัญญา และผู้ให้บริการภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร หรือไม่
		2.2 องค์กรมีการแบ่งภารกิจและกำหนดผู้รับผิดชอบของหน่วยงานด้าน IT สารสนเทศในการควบคุมการเข้าถึงข้อมูลและทรัพย์สินสารสนเทศอย่างชัดเจนและเหมาะสมหรือไม่
		2.3 องค์กรมีการระบุข้อตกลงการรักษาความลับข้อมูลสารสนเทศในเอกสารสัญญาจ้าง เอกสาร TOR ทุกประเภทที่เกี่ยวข้องกับโครงการด้านเทคโนโลยีสารสนเทศหรือไม่
		2.4 องค์กรมีและใช้ข้อมูลที่เป็นปัจจุบันในการติดต่อแลกเปลี่ยนเรียนรู้ด้านเทคโนโลยีสารสนเทศภัยคุกคามหรือจุดอ่อนกับ

ข้อ	หัวข้อมาตรฐาน ISO 27001:2013	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
		หน่วยงานที่มีความรอบรู้ ความชำนาญ ด้านความมั่นคงปลอดภัยหรือไม่
		2.5 องค์กรมีการกำหนดแนวทางการปฏิบัติงานจากระยะไกลเพื่อควบคุมการเข้าถึง การประมวลผล และจัดเก็บข้อมูลการใช้งานหรือไม่
		2.6 องค์กรมีการกำหนดนโยบายถึงแนวทางปฏิบัติสำหรับการใช้งานอุปกรณ์สื่อสารแบบพกพา โดยมีการแจ้งให้บุคลากรภายในและหน่วยงานภายนอกที่เกี่ยวข้องรับทราบหรือไม่
3	การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร	3.1 องค์กรมีการจัดเก็บข้อมูลบุคลากรโดยใช้ระบบเทคโนโลยีสารสนเทศ และมีนโยบายระเบียบ ข้อบังคับในการตรวจสอบประวัติการทำงานย้อนหลังก่อนรับสมัครบุคลากรเข้าทำงานในองค์กรหรือไม่
		3.2 องค์กรมีการกำหนดข้อตกลงในการจ้างงานที่ระบุให้ผู้รับจ้างปฏิบัติตามกฎ ระเบียบ และความรับผิดชอบด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรหรือไม่
		3.3 องค์กรมีการกำหนดให้บุคลากรในองค์กรปฏิบัติตามนโนบายด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและมีการกำกับดูแลตามสายบังคับบัญชาหรือไม่
		3.4 องค์กรมีการจัดฝึกอบรมเพื่อสร้างความตระหนัก รับรู้ เกี่ยวกับความมั่นคงปลอดภัยจากการใช้งานสารสนเทศและกระบวนการ

ข้อ	หัวข้อมาตรฐาน ISO 27001:2013	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
		ปฏิบัติงานอย่างสม่ำเสมอหรือไม่
		3.5 องค์กรมีระบบการตรวจสอบและระบุบทลงโทษทางวินัย หากมีการละเมิดหรือกระทำที่ทำให้องค์กรเกิดความเสี่ยง ความเสียหายต่อความมั่นคงปลอดภัยจากการใช้งานสารสนเทศหรือไม่
		3.6 องค์กรมีการกำหนดขั้นตอนการปฏิบัติด้านความมั่นคงปลอดภัย เมื่อพนักงานสิ้นสุดการจ้างหรือเปลี่ยนแปลงตำแหน่งงานและได้มีการดำเนินการตามนั้นหรือไม่
4	การบริหารจัดการทรัพย์สินสารสนเทศ	4.1 องค์กรมีการจัดทำบัญชีทรัพย์สินที่เกี่ยวข้องกับอุปกรณ์สารสนเทศและมีการอัพเดตข้อมูลเป็นปัจจุบันอย่างครบถ้วนสมบูรณ์หรือไม่
		4.2 รายการทรัพย์สินสารสนเทศองค์กรของท่านทุกรายการมีการระบุสถานที่จัดเก็บและผู้รับผิดชอบที่ชัดเจนหรือไม่
		4.3 องค์กรมีการกำหนดและตรวจสอบให้พนักงานคืนทรัพย์สินทั้งหมดที่ถือครองเมื่อสิ้นสุดการจ้างงานหรือเปลี่ยนแปลงตำแหน่งงานหรือไม่
		4.4 องค์กรมีนโยบายในการจัดชั้นความลับข้อมูลและกำหนดขั้นตอนการปฏิบัติงานจัดระดับชั้นความลับของข้อมูลหรือไม่
		4.5 องค์กรมีการกำหนดขั้นตอนในการปฏิบัติ จัดเก็บสารสนเทศได้อย่างเหมาะสมสอดคล้องกับประเภทของสารสนเทศหรือไม่
		4.6 องค์กรมีการกำหนดแนวทางการบริหาร

ข้อ	หัวข้อมาตรฐาน ISO 27001:2013	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
		จัดการขั้นตอนปฏิบัติการ และการทำลายข้อมูลบนสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้อย่างเหมาะสมและสอดคล้อง กับประเภทของสารสนเทศหรือไม่
		4.7 องค์กรมีการสำรองอุปกรณ์ประมวลผลสารสนเทศไว้อย่างเพียงพอตรงตามความต้องการ และมีความพร้อมในการใช้งาน?
5	การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ	5.1 องค์กรมีการจัดทำนโยบายควบคุมการเข้าถึงเครือข่าย และจัดให้มีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอหรือไม่ เช่น การบริหารจัดการรหัสผ่าน การพิสูจน์ตัวตน และการเข้าถึงศูนย์คอมพิวเตอร์
		5.2 องค์กรมีการกำหนดสิทธิ์ให้ผู้ใช้งานภายนอกสามารถเข้าถึงเครือข่ายและการบริการเครือข่ายขององค์กรหรือไม่
		5.3 องค์กรกำหนดขั้นตอนปฏิบัติการลงทะเบียนผู้ใช้งานใหม่และขั้นตอนปฏิบัติการถอดถอนสิทธิ์การใช้งานเมื่อออกจากองค์กรหรือไม่
		5.4 องค์มีการกำหนดระดับสิทธิ์การเข้าถึงระบบงาน ระบบปฏิบัติการ ระบบฐานข้อมูลหรือระบบงานอื่นๆ เหมาะสมต่อความจำเป็นของผู้ใช้งานแต่ละตำแหน่งหรือไม่
		5.5 องค์กรมีการอบรมให้ความรู้ แนวทางการกำหนดรหัสผ่านเกี่ยวกับการใช้งานด้านเทคโนโลยีสารสนเทศที่ปลอดภัยให้แก่บุคลากรในองค์กรหรือไม่
		5.6 องค์กรมีการกำหนดระยะเวลาสิ้นสุด

ข้อ	หัวข้อมาตรฐาน ISO 27001:2013	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
		การใช้งานของระบบงานเมื่อไม่มีกิจกรรมหรือมีการกำหนดระยะเวลาในการเชื่อมต่อระบบงานหรือไม่
		5.7 องค์กรมีนโยบายหรือข้อกำหนดการตรวจสอบควบคุมการใช้งานโปรแกรมอรรถประโยชน์นอกเหนือจากที่องค์กรกำหนดหรือไม่
6	การควบคุมการเข้ารหัสข้อมูล	6.1 องค์กรมีการกำหนดนโยบายการเข้าใช้งานรหัสข้อมูล และมีการตรวจสอบการใช้งานตามนโยบายหรือไม่
7	การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม	7.1 องค์กรมีการกำหนดขอบเขตหรือบริเวณโดยรอบทางกายภาพที่ต้องมีการรักษาความมั่นคงปลอดภัยการแบ่งแยกพื้นที่เหมาะสมหรือไม่
		7.2 องค์กรมีการควบคุมการเข้าออกของพื้นที่เฉพาะผู้ที่มีสิทธิ์หรือผู้ที่ได้รับอนุญาตและได้มีการจัดทำขั้นตอนปฏิบัติสำหรับเข้าออกศูนย์คอมพิวเตอร์ ศูนย์สารสนเทศ อีกทั้งวิธีการสื่อสารถึงผู้ที่เกี่ยวข้องทราบหรือไม่
		7.3 องค์กรมีการออกแบบการรักษาความมั่นคงปลอดภัย ทางกายภาพของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวกหน่วยงานสารสนเทศ และศูนย์คอมพิวเตอร์หรือไม่ เช่น มี Access Control หรือกล้องวงจรปิด เป็นต้น
		7.4 องค์กรมีการมี การป้องกันภัยทางธรรมชาติการโจมตีหรือการบุกรุกจากภายนอก อุบัติเหตุที่เหมาะสมและมีการ

ข้อ	หัวข้อมาตรฐาน ISO 27001:2013	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
		ตรวจสอบการใช้งานอย่างสม่ำเสมอหรือไม่ เช่น มีการติดตั้ง Fire Alarm, Air Condition, Smoke Detector, เครื่องตรวจวัดความชื้น, ถังดับเพลิง เป็นต้น
		7.5 องค์กรมีการจัดวางอุปกรณ์สารสนเทศได้อย่างเหมาะสม ปลอดภัย และกำหนดให้ผู้มีสิทธิ์เท่านั้นที่สามารถเข้าถึงอุปกรณ์ได้อย่างเหมาะสมหรือไม่
		7.6 องค์กรมีการป้องกันการหยุดชะงักของอุปกรณ์ขณะทำงาน เช่น มีการติดตั้งUPS สำรองไฟ ระบบควบคุมอุณหภูมิ และเครื่องกำเนิดไฟฟ้า เป็นต้น ในแต่ละส่วนงานหรือไม่
		7.7 องค์กรมีการจัด ทำ Label และ จัดระเบียบ สายไฟ สายสื่อสาร และสายเคเบิ้ล เพื่อไม่ก่อให้เกิดการขัดขวางการทำงาน ป้องกันการแทรกแซงสัญญาณหรือการทำให้เสียหายหรือไม่
		7.8 องค์กรมีการกำหนดขั้นตอนการปฏิบัติรักษาความปลอดภัยทรัพย์สินที่นำไปใช้งานนอกองค์กรหรือไม่
		7.9 องค์กรมีการกำหนดมาตรการป้องกันอุปกรณ์อมพิวเตอร์ที่ใช้งานขณะที่ไม่มีผู้ดูแลหรือการใช้งาน หรือไม่ เช่น มีการปิดหน้าจอและกำหนดการเข้ารหัสในการใช้งาน เป็นต้น
8	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ	8.1 องค์กรมีการกำหนดขั้นตอนปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรและเป็นปัจจุบันหรือไม่ เช่น ขั้นตอนการปฏิบัติงานในศูนย์

ข้อ	หัวข้อมาตรฐาน ISO 27001:2013	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
		คอมพิวเตอร์การสำรองข้อมูล การนำเข้าข้อมูลระบบในงาน การกู้คืนระบบ เป็นต้น
		8.2 องค์กรมีการตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ตั้งโต๊ะของบุคลากรในองค์กรหรือไม่ ว่ามีการติดตั้ง Anti-virus และตั้ง Auto Update รวมถึงการสร้างความตระหนักในการจัดการโปรแกรมไม่ประสงค์ดี
		8.3 องค์กรมีการกำหนดขั้นตอนการสำรองข้อมูลและรายงานผลการทดสอบข้อมูลที่สำรองต่อผู้บังคับบัญชาอย่างสม่ำเสมอ?
		8.4 องค์กรมีการกำหนดสิทธิการเข้าถึงอุปกรณ์บันทึกล็อคเฉพาะผู้มีสิทธิ์หรือไม่
		8.5 องค์กรมีการตั้งเวลาของระบบที่สำคัญทั้งหมดในองค์กรว่าถูกต้อง ตรงกันกับอุปกรณ์เทียบเวลาจากแหล่งอ้างอิง NTP Server หรือไม่
		8.6 องค์กรมีการติดตาม เฝ้าระวัง และประเมินความเสี่ยงช่องโหว่ที่เกิดขึ้น และมีมาตรการจัดการช่องโหวที่เกิดขึ้นอย่างเหมาะสม ทันเวลาหรือไม่
		8.7 องค์กรมีการตรวจสอบควบคุมการติดตั้งซอฟต์แวร์ ว่ามีความเหมาะสมและเป็นปัจจุบันหรือไม่
9	การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์	9.1 องค์กรมีการบริหารจัดการควบคุมเครือข่าย โดยแบ่งแยกโซนเครือข่าย และแบ่งแยก VLAN กลุ่มผู้ใช้งานหรือไม่
		9.2 องค์กรมีการกำหนดระดับของข้อตกลง

ข้อ	หัวข้อมาตรฐาน ISO 27001:2013	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
		ในการให้บริการเครือข่ายไว้อย่างเหมาะสม ทั้งการให้บริการภายในและภายนอกองค์กรหรือไม่
		9.3 องค์กรมีการกำหนดนโยบาย ขั้นตอนการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานภายนอกตลอดจนการรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูลสารสนเทศขององค์กรกับหน่วยงานภายนอกหรือไม่
10	การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ	10.1 องค์กรมีกระบวนการป้องกันข้อมูลสารสนเทศจากการถูกเปิดเผยหรือเปลี่ยนแปลงแก้ไข ข้อมูลโดยผู้ที่ไม่มีสิทธิ รวมถึงมีการวิเคราะห์ช่องโหว่หรือการทดสอบเจาะระบบการส่งข้อมูลผ่านเครือข่ายสาธารณะหรือไม่
		10.2 องค์กรมีกระบวนการป้องกันข้อมูลสารสนเทศบนธุรกรรมออนไลน์จากการรับส่งข้อมูลที่ไม่สมบูรณ์ ผิดเส้นทาง หรือมีการเปลี่ยนแก้ไขจากผู้ที่ไม่มีสิทธิหรือไม่
		10.3 องค์กรมีการกำหนดข้อตกลงในการพัฒนาระบบให้มีความมั่นคงปลอดภัย และมีการตรวจสอบว่ามีการปฏิบัติตามข้อตกลงหรือไม่
		10.4 องค์กรมีแนวทางการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ รวมถึงมีการทดสอบหลังการเปลี่ยนแปลง โดยได้รับการอนุมัติให้มีการประเมินผลกระทบจากผู้มีอำนาจและมีการรายงานผลทุกครั้งหรือไม่
		10.5 องค์กรมีการกำหนดหลักวิศวกรรม

ข้อ	หัวข้อมาตรฐาน ISO 27001:2013	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
		ระบบให้มีความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษรและเป็นปัจจุบันหรือไม่
11	การควบคุมดูแลผู้ให้บริการภายนอก	11.1 องค์กรมีแนวทางปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศระหว่างองค์กรกับผู้ให้บริการภายนอกหรือไม่ เช่น การกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก เป็นต้น
		11.2 องค์กรมีการทำสัญญาจ้างกับผู้ให้บริการภายนอก โดยมีข้อกำหนดในการควบคุมการดำเนินงานของผู้ให้บริการภายนอกและผู้ที่เกี่ยวข้องต้องปฏิบัติตามข้อกำหนดขององค์กรหรือไม่
		11.3 องค์กรมีการติดตามและทบทวนการให้บริการของผู้ให้บริการภายนอก โดยมีการประเมินผลการให้บริการและรายงานแก่หัวหน้าหรือผู้บังคับบัญชาหรือไม่
12	การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	12.1 องค์กรมีการกำหนดขั้นตอนการรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมหรือไม่
		12.2 องค์กรมีการกำหนดเกณฑ์ประเมินสถานการณ์ความมั่นคงปลอดภัยจากเหตุการณ์ที่ ไม่พึงประสงค์และวิธีแก้ไขเหตุขัดข้องหรือไม่
		12.3 องค์กรมีการจัดทำสรุปจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยเพื่อหาแนวทางในการแก้ไขระยะยาวหรือไม่
		12.4 องค์กรมีการระบุ รวบรวม จัดหาและจัดเก็บหลักฐานข้อมูลสารสนเทศ เมื่อเกิด

ข้อ	หัวข้อมาตรฐาน ISO 27001:2013	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
		เหตุการณ์ที่มีความเกี่ยวข้องกับการดำเนินการทางกฎหมายหรือไม่
13	การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	13.1 องค์กรมีข้อกำหนดสำหรับความมั่นคงปลอดภัยสารสนเทศและความต่อเนื่องเพื่อบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในสถานการณ์ร้ายแรงหรือไม่ เช่น การวางแผนเตรียมการสภาพความพร้อมใช้ของระบบงานในนโยบาย ว่ามีการประเมินผลกระทบทางธุรกิจกรณีระบบงานหยุดชะงักและกำหนดระดับความสำคัญของระบบงานหรือไม่
		13.2 องค์กรมีการเตรียมสำรองอุปกรณ์ประมวลผลสารสนเทศไว้อย่างเพียงพอตรงตามความต้องการและมีความพร้อมใช้งาน ได้รับการบำรุงรักษาอย่างเหมาะสม และมีสำรองกรณี ชำรุดเสียหายไม่ สามารถซ่อมได้
14	การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด (ความสอดคล้อง)	14.1 องค์กรมีการจัดทำรายการข้อกฎหมายด้านความมั่นคงปลอดภัยสารสนเทศรวมถึงข้อกำหนดขององค์กรที่ต้องปฏิบัติไว้เป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบัน อีกทั้งได้มีการเผยแพร่ให้คนในองค์กรทราบอย่างทั่วถึงหรือไม่
		14.2 องค์กรมีการจัดทำขั้นตอนการจัดการลิขสิทธิ์ซอฟต์แวร์ และมีการบริหารจัดการลิขสิทธิ์ซอฟต์แวร์ อย่างเหมาะสมหรือไม่
		14.3. องค์กรมีการระบุระดับชั้นความลับของข้อมูล การทำป้ายแสดงระดับชั้นความลับและการจัดการสารสนเทศตามนโยบาย

ข้อ	หัวข้อมาตรฐาน ISO 27001:2013	ข้อคำถามใหม่ที่ได้จากการอ้างอิงมาตรฐาน
		องค์กรหรือไม่
		14.4 องค์กรมีการทบทวนการเนินการด้านความมั่นคงปลอดภัยสารสนเทศโดยผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกเป็นประจำตามรอบระยะเวลาที่กำหนดหรือไม่
		14.5. องค์กรมีการทบทวนโยบายความมั่นคงปลอดภัยสารสนเทศโดยการอ้างอิงมาตรฐาน ISO 27001 ฉบับปัจจุบันหรือไม่

ภาคผนวก ค

แบบสอบถามเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศในองค์กร

แบบสอบถาม ข้อมูลทั่วไปเกี่ยวกับการใช้งานสารสนเทศในองค์กร

(สำหรับเจ้าหน้าที่ดูแลจัดการระบบสารสนเทศองค์กร)

วัตถุประสงค์ เพื่อสำรวจและเก็บข้อมูลพฤติกรรมการใช้งานเทคโนโลยีสารสนเทศที่ก่อให้เกิดความเสี่ยงไม่ปลอดภัยของข้อมูลในองค์กร และนำไปวิเคราะห์เพื่อพัฒนาระบบประเมินความเสี่ยงของผู้ใช้เทคโนโลยีสารสนเทศในองค์กรต่อไป

แบบสอบถามแบ่งออกเป็น 2 ส่วน กรุณาทำเครื่องหมาย √ ลงหน้าข้อคำตอบที่เกี่ยวข้องกับท่าน

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

1. **ตำแหน่งงานปัจจุบันของคุณคือ**
   - ☐ เจ้าหน้าที่ดูแลเกี่ยวกับระบบสารสนเทศองค์กร
   - ☐ เจ้าหน้าที่ปฏิบัติงานทั่วไป
   - ☐ ครู-อาจารย์
   - ☐ อื่นๆ ระบุ.....
2. **ปัจจุบันคุณมีอายุ**
   - ☐ ระหว่าง 18-29 ปี ☐ ระหว่าง 30-44 ปี
   - ☐ ระหว่าง 45-59 ปี ☐ มากกว่า 59 ปีขึ้นไป
3. **เพศ** ☐ ชาย ☐ หญิง
4. **วุฒิการศึกษาสูงสุด**
   - ☐ ต่ำกว่าปริญญาตรี
   - ☐ ระดับปริญญาตรี
   - ☐ ระดับปริญญาโท
   - ☐ ระดับปริญญาเอก

5. ประสบการณ์ในการทำงานด้านเทคโนโลยีสารสนเทศ

☐ น้อยกว่า 3 ปี ☐ 5-10 ปี ☐ 11-15 ปี ☐ 16-20 ปี ☐ มากกว่า 20 ปี

ส่วนที่ 2 สำหรับเจ้าหน้าที่ผู้ดูแลระบบสารสนเทศในองค์กร หรือผู้มีส่วนเกี่ยวข้องในการบริหารจัดการกับระบบสารสนเทศในองค์กร อ้างอิงจากโครงสร้างมาตรฐาน ISO 27001:2013 แบ่งเนื้อหาออกเป็น 14 ด้าน

ด้านที่ 1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

1.1 องค์กรมีการจัดทำนโยบาย ความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษรและได้รับอนุมัติจากผู้บริหารรวมทั้งมีการสื่อสารให้บุคลากรในองค์กรรับทราบหรือไม่

- ☐ 1. มีการจัดทำนโยบายเป็นลายลักษณ์อักษรโดยมีผู้บริหารเป็นผู้อนุมัติและประกาศเผยแพร่แก่บุคลากรรับทราบโดยทั่วกัน
- ☐ 2. มีการจัดทำนโยบายและมีการประกาศให้บุคลากรในองค์กรได้รับทราบ แต่อาจไม่ทั่วถึงทุกส่วนงานในองค์กร
- ☐ 3. มีการจัดทำนโยบายแต่ไม่ได้มีการประกาศให้ทราบร่วมกันแต่อย่างใด
- ☐ 4. บุคลากรไม่ทราบว่ามีนโยบายหรือไม่ เพราะไม่มีการประกาศและไม่ได้สนใจเรื่องนี้
- ☐ 5. ไม่มีการจัดทำนโยบายความความมั่นคงปลอดภัยฯ

1.2 นโยบายความมั่นคงปลอดภัยสารสนเทศ มีเนื้อหาที่เหมาะสม ครบถ้วนเพียงพอ และได้รับการทบทวนตามรอบระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงหรือไม่

- ☐ 1. นโยบายมีเนื้อหาที่เหมาะสม ครบถ้วนเพียงพอ มีความเป็นปัจจุบัน และได้รับการปรับปรุงตามรอบระยะเวลาหรือช่วงที่สถานการณ์มีการเปลี่ยนแปลงเสมอ
- ☐ 2. นโยบายมีเนื้อหาที่เหมาะสม เพียงพอสำหรับในองค์กร แต่ไม่ค่อยได้รับการทบทวนให้เป็นปัจจุบัน
- ☐ 3. เนื้อหาข้อมูลในนโยบายมีไม่เพียงพอสำหรับในองค์กร และไม่ได้รับการทบทวนให้เป็นปัจจุบันเท่าไหร่

- 4. มีนโยบายแต่ไม่แน่ใจว่าเนื้อหาข้อมูลมีความเหมาะสมเพียงพอและมีการทบทวนให้เป็นปัจจุบันหรือไม่อย่างไร
- 5. องค์กรไม่มีนโนบายที่เกี่ยวข้องแต่อย่างใด

<u>ด้านที่ 2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ</u>

2.1 องค์กรมีการกำหนดขอบเขตและมอบหมายหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศให้แก่พนักงานภายในองค์กร คู่สัญญา และผู้ให้บริการภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร หรือไม่

- 1. มีการประกาศกำหนดขอบเขตความรับผิดชอบที่ชัดเจนทั้งวาจาและลายลักษณ์อักษรให้พนักงานในองค์กรคู่สัญญาและบุคคลภายนอกทราบ
- 2. มีการประกาศกำหนดขอบเขตความรับผิดชอบที่ชัดเจน ทั้งวาจาและลายลักษณ์อักษรให้พนักงานในองค์กรและคู่สัญญารับทราบ
- 3. มีการประกาศกำหนดขอบเขตความรับผิดชอบที่ชัดเจน ทั้งวาจาและลายลักษณ์อักษรให้พนักงานในองค์กรรับทราบ
- 4. มีการประกาศกำหนดขอบเขตความรับผิดชอบด้วยวาจาหรือเป็นลายลักษณ์อักษรเฉพาะพนักงานในองค์กรหรือคู่สัญญาหรือบุคลากรภายนอกให้รับทราบเท่านั้น
- 5. ไม่มีการดำเนินการจัดทำใดๆ

2.2 องค์กรมีการแบ่งภารกิจและกำหนดผู้รับผิดชอบของหน่วยงานด้าน IT สารสนเทศในการควบคุมการเข้าถึงข้อมูลและทรัพย์สินสารสนเทศอย่างชัดเจนและเหมาะสมหรือไม่

- 1. หน่วยงานแบ่งภารกิจและกำหนดเจ้าหน้าที่ผู้รับผิดชอบอย่างชัดเจนและเหมาะสม
- 2. มีการแบ่งภารกิจที่ชัดเจน แต่กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบต้องปฏิบัติงานที่ซ้ำซ้อนกัน
- 3. หน่วยงานแบ่งภารกิจและกำหนดเจ้าหน้าที่ผู้รับผิดชอบไม่ชัดเจนทำให้การปฏิบัติงานไม่เป็นในทิศทางเดียวกัน สับสนมีความซ้ำซ้อน
- 4. หน่วยงานไม่มีการแบ่งภารกิจและกำหนดเจ้าหน้าที่ผู้รับผิดชอบให้ชัดเจนแต่ให้ช่วยกันทำ
- 5. ไม่มีการดำเนินการใดๆ

2.3 องค์กรมีการระบุข้อตกลงการรักษาความลับข้อมูลสารสนเทศในเอกสารสัญญาจ้าง เอกสาร TOR ทุกประเภทที่เกี่ยวข้องกับโครงการด้านเทคโนโลยีสารสนเทศหรือไม่

- ☐ 1. มีการระบุข้อตกลงการรักษาความลับข้อมูลสารสนเทศในเอกสารสัญญาและเอกสารทุกประเภทที่เกี่ยวข้องกับโครงการด้าน IT สารสนเทศกับบุคคลภายในและบุคคลภายนอก
- ☐ 2. มีการระบุข้อตกลงการรักษาความลับข้อมูลสารสนเทศในเอกสารสัญญาและเอกสารทุกประเภทที่เกี่ยวข้องกับโครงการด้าน IT สารสนเทศกับบุคคลภายนอกเท่านั้น
- ☐ 3. มีแต่การระบุข้อตกลแนวทางการปฏิบัติ ระยะเวลา การดำเนินงาน แต่ไม่มีที่เกี่ยวกับการรักษาความลับข้อมูลสารสนเทศขององค์กร
- ☐ 4. มีแน่ใจว่ามีหรือไม่ แต่เหมือนจะเคยเห็นไม่แน่ใจ
- ☐ 5. ไม่มีการระบุหรือดำเนินการที่เกี่ยวกับการรักษาความลับข้อมูลแต่อย่างใด

2.4 องค์กรมีและใช้ข้อมูลที่เป็นปัจจุบันในการติดต่อแลกเปลี่ยนเรียนรู้ด้านเทคโนโลยีสารสนเทศภัยคุกคามหรือจุดอ่อนกับหน่วยงานที่มีความรอบรู้ ความชำนาญ ด้านความมั่นคงปลอดภัยหรือไม่

- ☐ 1. หน่วยงานมีข้อมูลที่เป็นปัจจุบันและการติดต่อหรือขอรับคำปรึกษาเพื่อแก้ไขปัญหากับหน่วยงานทุกครั้ง
- ☐ 2. หน่วยงานมีข้อมูลที่เป็นปัจจุบันและใช้ติดต่อหรือขอรับคำปรึกษาเพื่อแก้ไขปัญหากับหน่วยงานทุกครั้ง
- ☐ 3. มีข้อมูลที่เกี่ยวข้องแต่ยังไม่มีการปรับปรุงข้อมูลให้เป็นปัจจุบันและไม่เคยมีการติดต่อกับหน่วยงาน
- ☐ 4. เคยมีการจัดทำข้อมูลและติดต่อหน่วยงานแต่ไม่มีการปรับปรุงข้อมูลให้เป็นปัจจุบัน
- ☐ 5. ไม่มีการจัดทำข้อมูลขององค์กรและข้อมูลของหน่วยงานที่เกี่ยวข้องความปลอดภัยด้านเทคโนโลยีสารสนเทศไว้เลย

2.5 องค์กรมีการกำหนดแนวทางการปฏิบัติงานจากระยะไกลเพื่อควบคุมการเข้าถึง การประมวลผลและจัดเก็บข้อมูลการใช้งานหรือไม่

- ☐ 1. องค์กรมีการกำหนดการปฏิบัติงานจากระยะไกลที่ใช้ในการควบคุมการเข้าถึงการประมวลผลและมีการจัดเก็บข้อมูลการปฏิบัติงานทุกครั้ง
- ☐ 2. องค์กรมีการกำหนดแนวทางการปฏิบัติงานจากระยะไกลที่ใช้ในการควบคุมการเข้าถึงการประมวลผลแต่ไม่มีการจัดเก็บข้อมูลการเข้าถึง

- 3. องค์กรมีการกำหนดแนวทางการปฏิบัติงานจากระยะไกลแต่ไม่มีการประมวลผลและการจัดเก็บข้อมูลการเข้าถึง
- 4. องค์กรไม่มีการกำหนดแนวทางการปฏิบัติงาน มีแต่เจ้าหน้าที่ที่ปฏิบัติงานเองกรณีที่ต้องมีการปฏิบัติงานจากระยะไกล และไม่มีการจัดเก็บข้อมูลใดๆ
- 5. ไม่มีการกำหนดแนวทางปฏิบัติแต่อย่างใด

2.6 องค์กรมีการกำหนดนโยบายถึงแนวทางปฏิบัติสำหรับการใช้งานอุปกรณ์สื่อสารแบบพกพา โดยมีการแจ้งให้บุคลากรภายในและหน่วยงานภายนอกที่เกี่ยวข้องรับทราบหรือไม่

- 1. มีการกำหนดเป็นนโยบายและแนวทางการปฏิบัติพร้อมทั้งแจ้งประกาศให้บุคลากรภายในและหน่วยงานภายนอกองค์กรที่เกี่ยวข้องได้รับทราบและถือปฏิบัติโดยทั่วกัน
- 2. มีการกำหนดเป็นนโยบายและแนวทางการปฏิบัติ แต่แจ้งให้เฉพาะบุคลากรภายในองค์กรได้รับทราบและปฏิบัติเท่านั้น
- 3. มีการกำหนดเฉพาะแนวทางการปฏิบัติภายในองค์กรเท่านั้น
- 4. นโยบายและแนวทางปฏิบัติไม่สนับสนุนหรือเกื้อกูลซึ่งกันและกัน
- 5. ไม่มีแนวทางการกำหนดนโยบายแต่อย่างใด

<u>ด้านที่ 3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร</u>

3.1 องค์กรมีการจัดเก็บข้อมูลบุคลากรโดยใช้ระบบเทคโนโลยีสารสนเทศ และมีนโยบาย ระเบียบข้อบังคับในการตรวจสอบประวัติการทำงานย้อนหลังก่อนรับสมัครบุคลากรเข้าทำงานในองค์กรหรือไม่

- 1. องค์กรมีการจัดเก็บข้อมูลบุคลากร โดยใช้ระบบเทคโนโลยีสารสนเทศ และมีนโยบายให้ฝ่ายบุคลากรตรวจสอบประวัติการทำงานย้อนหลังก่อนการรับบุคลากรเข้าเข้างาน
- 2. องค์กรมีใช้การจัดเก็บข้อมูลบุคลากร โดยใช้ระบบเทคโนโลยีสารสนเทศและมีนโยบายในเรื่องการตรวจสอบประวัติการทำงานย้อนหลังแต่ไม่ค่อยได้ทำ
- 3. องค์กรมีการจัดเก็บข้อมูลบุคลากรในองค์กรโดยใช้ระบบเทคโนโลยีสารสนเทศแต่ไม่มีนโยบายในเรื่องการตรวจสอบประวัติการทำงานย้อนหลัง
- 4. ทราบแต่องค์กรมีนโยบายในการตรวจสอบประการวัติการรับบุคลากรเข้าทำงานส่วนการดำเนินงานไม่ทราบรายละเอียด
- 5. องค์กรไม่มีการใช้ IT ในการจัดเก็บข้อมูลบุคคลและตรวจสอบประวัติการทำงานย้อนหลัง

3.2 องค์กรมีการกำหนดข้อตกลงในการจ้างงานที่ระบุให้ผู้รับจ้างปฏิบัติตามกฎ ระเบียบ และความรับผิดชอบด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรหรือไม่

- 1. มีการกำหนดข้อตกลงในการจ้างงานที่ระบุความรับผิดชอบในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงให้บุคลากรเซ็นรับทราบแนวทางปฏิบัติพร้อมแสดงความยินยอมให้ลงโทษทางวินัยหากมีการฝ่าฝืนหรือไม่ปฏิบัติตามกฎ
- 2. มีการกำหนดข้อตกลงในการจ้างงานที่ระบุความรับผิดชอบในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรแต่ไม่ให้บุคลากรเซ็นรับทราบแนวทางปฏิบัติ พร้อมยินยอมให้ลงโทษทางวินัยหากมีการฝ่าฝืนหรือไม่ปฏิบัติตามกฎ
- 3. มีการกำหนดข้อตกลงแต่ไม่มีรายละเอียดความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศในองค์กรและไม่ได้ระบุแนวทางปฏิบัติหากไม่ทำตามข้อตกลง
- 4. ทราบว่ามีการจัดทำข้อตกลงระหว่างผู้ปฏิบัติงานกับองค์กรแต่ไม่ระบุรายละเอียดเกี่ยวกับความปลอดภัยด้านเทคโนโลยีสารสนเทศ
- 5. ไม่มีการกำหนดข้อตกลง

3.3 องค์กรมีการกำหนดให้บุคลากรในองค์กรปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและมีการกำกับดูแลตามสายบังคับบัญชาหรือไม่

- 1. มีนโยบายให้บุคลากรปฏิบัติงานตามข้อกำหนดด้านความมั่นคงปลอดภัยและให้ผู้บังคับบัญชากำกับดูแลตามสายงานที่รับผิดชอบ
- 2. มีแต่นโยบายให้บุคลากรปฏิบัติงานตามข้อกำหนดด้านความมั่นคงปลอดภัยและกำกับดูแลในภาพรวมขององค์กรเท่านั้น
- 3. มีแต่วิธีปฏิบัติและการใช้งานเทคโนโลยีสารสนเทศให้มีความปลอดภัยมีการกำกับดูแลในภาพรวมขององค์กรที่ไม่ใช่เฉพาะสายงาน
- 4. มีนโยบายที่เกี่ยวข้องแต่ไม่ครอบคลุมทั้งหมดและไม่มีการกำกับดูแลจากผู้บังคับบัญชาจากสายงานแต่อย่างใด
- 5. ไม่มีนโนบายหรือข้อกำหนดที่เกี่ยวข้องกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและไม่มีการกำกับดูแลจากผู้บังคับบัญชาสายงานแต่อย่างใด

3.4 องค์กรมีการจัดฝึกอบรมเพื่อสร้างความตระหนัก รับรู้ เกี่ยวกับความมั่นคงปลอดภัยจากการใช้งานสารสนเทศและกระบวนการปฏิบัติงานอย่างสม่ำเสมอหรือไม่

- 1. มีการจัดอบรมให้ความรู้แก่บุคลากรอย่างสม่ำเสมอ เป็นปัจจุบันและสอดคล้องกับสถานการณ์ที่มีการเปลี่ยนแปลงทางด้านเทคโนโลยี
- 2. มีการจัดอบรม ปีละ 1–2 ครั้ง
- 3. มีการจัดอบรมปีเว้นปี
- 4. ยังไม่เคยมีมาก่อน แต่กำลังจะมีการจัดอบรมให้เร็วๆ นี้
- 5. องค์กรยังไม่มีการจัดอบรมเกี่ยวกับด้านนี้เลยสักครั้ง

3.5 องค์กรมีระบบการตรวจสอบและระบุบทลงโทษทางวินัย หากมีการละเมิดหรือกระทำที่ทำให้องค์กรเกิดความเสี่ยง ความเสียหายต่อความมั่นคงปลอดภัยจากการใช้งานสารสนเทศหรือไม่

- 1. มีการตรวจสอบและระบุบทลงโทษ ไว้อย่างชัดเจนและมีการดำเนินอย่างจริงจังหากพบผู้ละเมิด
- 2. มีการระบุบทลงโทษ ไว้อย่างชัดเจนมีการตรวจสอบแต่ไม่มีการดำเนินบทลงโทษที่จริงจัง
- 3. มีการระบุบทลงโทษไว้อย่างชัดเจน แต่ขาดการตรวจสอบและการดำเนินการอย่างจริงจังสำหรับผู้กระทำการละเมิด
- 4. เคยมีการระบุบทลงโทษแต่ข้อมูลดังกล่าวยังไม่ได้รับการปรับให้เป็นปัจจุบันและหลังจากนั้นก็ไม่มีการตรวจสอบหรือดำเนินการใดๆ อีกเลย
- 5. ไม่มีระบบการตรวจสอบหรือระบุบทลงโทษไว้แต่อย่างใด

3.6 องค์กรมีการกำหนดขั้นตอนการปฏิบัติด้านความมั่นคงปลอดภัย เมื่อพนักงานสิ้นสุดการจ้างหรือเปลี่ยนแปลงตำแหน่งงาน และได้มีการดำเนินการตามนั้นหรือไม่

- 1. มีการกำหนดขั้นตอนการปฏิบัติงานเมื่อบุคลากรสิ้นสุดหรือเปลี่ยนตำแหน่งงานนั้นๆ และมีการดำเนินการตามขั้นตอนการปฏิบัติงานด้านความมั่นคงปลอดภัยทุกครั้ง
- 2. มีการกำหนดขั้นตอนการปฏิบัติงานด้านความมั่นคงปลอดภัย แต่ไม่ได้ดำเนินการตามขั้นตอนทุกกรณี
- 3. ไม่มีการกำหนดขั้นตอนการปฏิบัติงานด้านความมั่นคงปลอดภัยแต่จะมีการลงโทษเมื่อพบผู้กระทำการละเมิดตามที่องค์กรเห็นสมควร

- 4. ไม่ทราบข้อมูลในส่วนนี้ เนื่องจากเป็นหน้าที่ของฝ่ายบุคลากร
- 5. ไม่มีการกำหนดขั้นตอนหรือการปฏิบัติที่เกี่ยวข้องกับการปฏิบัติด้านความมั่นคงปลอดภัยเมื่อสิ้นสุดการจ้างหรือเปลี่ยนแปลงตำแหน่งงานในองค์กร

ด้านที่ 4 การบริหารจัดการทรัพย์สินสารสนเทศ

4.1 องค์กรมีการจัดทำบัญชีทรัพย์สินที่เกี่ยวข้องกับอุปกรณ์สารสนเทศและมีการอัพเดตข้อมูลเป็นปัจจุบันอย่างครบถ้วนสมบูรณ์หรือไม่

- 1. มีการจัดทำรายการบัญชีทรัพย์สิน วัสดุอุปกรณ์ของสำนักงานทุกชิ้นรวมไปถึงที่เกี่ยวข้องกับด้านสารสนเทศด้วย มีการอัพเดตรายการบัญชีเป็นปัจจุบันล่าสุด
- 2. มีการจัดทำรายการบัญชีทรัพย์สิน วัสดุอุปกรณ์ของสำนักงานแต่ยังไม่ได้ทำการอัพเดตข้อมูลเป็นปัจจุบัน
- 3. มีการจัดทำรายการบัญชีทรัพย์สิน วัสดุอุปกรณ์ของสำนักงานและสารสนเทศแต่ไม่ครบทุกรายการ ไม่แน่ใจมีการอัพเดตเป็นปัจจุบันหรือไม่
- 4. มีแต่การจัดทำรายการบัญชีพัสดุทั่วไป ไม่พบการจัดทำบัญชีที่เกี่ยวกับสารสนเทศ
- 5. ไม่มีการจัดทำรายการบัญชีทรัพย์สินที่เกี่ยวข้องในด้านสารสนเทศหรืออุปกรณ์ต่างๆของสำนักงานแต่อย่างใด

4.2 รายการทรัพย์สินสารสนเทศองค์กรของท่านทุกรายการมีการระบุสถานที่จัดเก็บและผู้รับผิดชอบที่ชัดเจนหรือไม่

- 1. รายการทรัพย์สินสารสนเทศทุกรายการมีการระบุสถานที่จัดเก็บและผู้รับผิดชอบที่ชัดเจนและมีการตรวจสอบสม่ำเสมอ
- 2. รายการทรัพย์สินสารสนเทศมีการระบุสถานที่จัดเก็บผู้รับผิดชอบมีการตรวจสอบบ้างนานๆครั้ง
- 3. รายการทรัพย์สินสารสนเทศมีผู้รับผิดชอบแต่ไม่ได้รับการตรวจสอบ
- 4. มีการทำบัญชีทรัพย์สินเป็นภาพรวมไม่ได้เฉพาะด้านสารสนเทศข้อมูลจึงไม่ครบถ้วน
- 5. ไม่มีการจัดทำบัญชีหรือระบุผู้รับผิดชอบและตรวจสอบแต่อย่างใด

4.3 องค์กรมีการกำหนดและตรวจสอบให้พนักงานคืนทรัพย์สินทั้งหมดที่ถือครองเมื่อสิ้นสุดการจ้างงานหรือเปลี่ยนแปลงตำแหน่งงานหรือไม่

- 1. มีการกำหนดและตรวจสอบทรัพย์สินขององค์กรตั้งแต่พนักงานเข้าทำงานจนถึงวันที่พนักงานสิ้นสุดการทำงานกับองค์กรจะมีการตรวจสอบอีกครั้งก่อนการอนุมัติให้ออก

- 2. มีการกำหนดและตรวจสอบทรัพย์สินเฉพาะกรณีที่สิ้นสุดการจ้างงานส่วนการมีการเปลี่ยนแปลงตำแหน่งงานภายในไม่มีการตรวจสอบ
- 3. มีการกำหนดไว้แต่ไม่ค่อยมีการปฏิบัติอย่างจริงจังครบทุกคนเมื่อถึงเวลาสิ้นสุดการเป็นพนักงานหรือบุคลากรขององค์กร
- 4. ไม่แน่ใจว่ามีหรือไม่แต่เห็นมีการตรวจสอบบ้างเป็นบางรายบุคคล
- 5. ไม่มีการกำหนดและตรวจสอบใดๆเมื่อพนักงานหรือบุคลากรสิ้นสุดการทำงานร่วมกับองค์กร

4.4 องค์กรมีนโยบายในการจัดชั้นความลับข้อมูลและกำหนดขั้นตอนการปฏิบัติงานจัดระดับชั้นความลับของข้อมูลหรือไม่

- 1. มีการกำหนดนโยบายกำหนดขั้นตอนในการปฏิบัติงานและกำหนดระดับชั้นความลับของข้อมูลไว้อย่างชัดเจน
- 2. มีการกำหนดนโยบาย การจัดลำดับชั้นของข้อมูล และกำหนดขั้นตอนในการปฏิบัติงานเฉพาะบางส่วนงานที่เห็นว่าสมควรเท่านั้น
- 3. ไม่มีการกำหนดนโยบายหรือกำหนดขั้นตอนปฏิบัติให้กับผู้ปฏิบัติงานมีเพียงหัวหน้างานเท่านั้นที่จะได้รับมอบหมายให้ดำเนินการดังกล่าวผ่านทางผู้บริหาร
- 4. ไม่มีการกำหนดนโยบายหรือขั้นตอนการปฏิบัติ แต่มีการแจ้งด้วยวาจาให้ผู้ปฏิบัติงานบางคนดำเนินการจัดระดับชั้นความลับข้อมูลเท่านั้น
- 5. ไม่มีการกำหนดนโยบายหรือขั้นตอนในการปฏิบัติดังกล่าว

4.5 องค์กรมีการกำหนดขั้นตอนในการปฏิบัติ จัดเก็บสารสนเทศได้อย่างเหมาะสม สอดคล้องกับประเภทของสารสนเทศหรือไม่

- 1. มีการกำหนดขั้นตอนและการจัดเก็บสารสนเทศได้อย่างสอดคล้องและเหมาะสมกับประเภทของสารสนเทศ
- 2. มีการกำหนดขั้นตอนและสอดคล้องกับประเภทของสารสนเทศแต่ยังไม่มีการจัดเก็บที่เหมาะสม
- 3. ไม่มีการกำหนดขั้นตอนการปฏิบัติในการจัดเก็บมีแต่การจัดเก็บที่ไม่ได้ทำการแยกประเภทซึ่งยังไม่เหมาะสมในการจัดเก็บเท่าที่ควร
- 4. เคยมีการกำหนดขั้นตอนการปฏิบัติที่ไม่เหมาะสมและไม่สอดคล้องกับประเภทใน

การจัดเก็บซึ่งยังไม่ได้รับการปรับปรุงให้มีความเหมาะสมเท่าที่ควร

- 5. ไม่มีการกำหนดขั้นตอนและการจัดเก็บสารสนเทศที่เหมาะสมและสอดคล้องกับประภทของสารสนเทศ

4.6 องค์กรมีการกำหนดแนวทางการบริหารจัดการขั้นตอนปฏิบัติการ และการทำลายข้อมูลบนสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้อย่างเหมาะสมและสอดคล้อง กับประเภทของสารสนเทศหรือไม่

- 1. มีการกำหนดขั้นตอนและการจัดเก็บสารสนเทศได้อย่างสอดคล้องและเหมาะสมกับประเภทของสารสนเทศ
- 2. มีการกำหนดขั้นตอนและสอดคล้องกับประเภทของสารสนเทศแต่ยังไม่มีการจัดเก็บที่เหมาะสม
- 3. ไม่มีการกำหนดขั้นตอนการปฏิบัติในการจัดเก็บมีแต่การจัดเก็บที่ไม่ได้ทำการแยกประเภทซึ่งยังไม่เหมาะสมในการจัดเก็บเท่าที่ควร
- 4. เคยมีการกำหนดขั้นตอนการปฏิบัติที่ไม่เหมาะสมและไม่สอดคล้องกับประเภทในการจัดเก็บซึ่งยังไม่ได้รับการปรับปรุงให้มีความเหมาะสมเท่าที่ควร
- 5. ไม่มีการกำหนดขั้นตอนและการจัดเก็บสารสนเทศ

4.7 องค์กรมีการสำรองอุปกรณ์ประมวลผลสารสนเทศไว้อย่างเพียงพอตรงตามความต้องการและมีความพร้อมในการใช้งานหรือไม่

- 1. มีการสำรองอุปกรณ์ไว้อย่างเพียงพอและมีความพร้อมในการใช้งาน
- 2. มีการสำรองอุปกรณ์ไว้ทุกส่วนงานแต่ไม่แน่ใจว่าเพียงพอหรือไม่เมื่อมีเหตุจำเป็น
- 3. มีการสำรองอุปกรณ์ไว้บ้างเฉพาะบางส่วนงาน และไม่แน่ใจว่ามีความพร้อมในการใช้งานมากน้อยเพียงใด
- 4. ไม่มีการสำรองอุปกรณ์ไว้หากส่วนงานไหนมีความต้องการให้ดำเนินการทำแผนโครงการหรือเบิกอุปกรณ์กันเอง
- 5. ไม่มีการสำรองอุปกรณ์ไว้เลย

<u>ด้านที่ 5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ</u>

5.1 องค์กรมีการจัดทำนโยบายควบคุมการเข้าถึงเครือข่าย และจัดให้มีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอหรือไม่ เช่น การบริหารจัดการรหัสผ่าน การพิสูจน์ตัวตน และการเข้าถึงศูนย์คอมพิวเตอร์

- 1. มีการควบคุมการเข้าถึงและมีการทบทวนสิทธิ์อย่างสม่ำเสมอ
- 2. มีการควบคุมการเข้าถึงและมีการทบทวนสิทธิ์บ้างเป็นบางครั้ง
- 3. มีการควบคุมการเข้าถึงแต่ไม่ได้มีการทบทวนสิทธิ์เลย
- 4. ไม่มีการควบคุมการเข้าถึงมีแต่ขั้นตอนในการใช้งานเครือข่ายเท่านั้นไม่มีการตรวจสอบสิทธิ์
- 5. ไม่มีการควบคุมการเข้าถึงและไม่มีการทบทวนสิทธิ์

5.2 องค์กรมีการกำหนดสิทธิ์ให้ผู้ใช้งานภายนอกสามารถเข้าถึงเครือข่ายและการบริการเครือข่ายขององค์กรหรือไม่

- 1. องค์กรมีการกำหนดรหัสผู้ใช้งานสามารถเข้าถึงเครือข่ายที่กำหนดไว้เท่านั้นและต้องได้รับการลงทะเบียนอุปกรณ์การเข้าใช้งานขอสิทธิ์ใช้ในการเข้าถึงทุกครั้ง
- 2. องค์กรมีการกำหนดสิทธิ์ในการเข้าถึงเครือข่ายโดยทำการลงทะเบียนขอใช้สิทธิ์และอุปกรณ์การเข้าใช้งานโดยอายุในการเข้าใช้งานเพียง 7 วัน ต่อรหัสเข้าใช้งานเท่านั้น
- 3. องค์กรมีการกำหนดสิทธิ์ในการเข้าถึงเครือข่ายโดยทำการลงทะเบียนขอใช้สิทธิ์และอุปกรณ์การเข้าใช้งานเพียงครั้งแรกที่เข้าใช้งานเท่านั้น
- 4. ไม่มีการกำหนดสิทธิ์หรือลงทะเบียนอุปกรณ์การเข้าใช้งานแต่อย่างใดหากจะเข้าใช้งานเครือข่ายต้องรอรับรหัสการเข้าใช้งานจากฝ่ายไอทีเป็นรายวันเท่านั้น
- 5. ไม่มีการกำหนดสิทธิ์เข้าใช้งานแต่อย่างใดสามารถเชื่อมต่อเข้าใช้งานได้ทันที

5.3 องค์กรกำหนดขั้นตอนปฏิบัติการลงทะเบียนผู้ใช้งานใหม่และขั้นตอนปฏิบัติการถอดถอนสิทธิ์การใช้งานเมื่อออกจากองค์กรหรือไม่

- 1. มีการกำหนดขั้นตอนการปฏิบัติและขั้นตอนในการถอดถอนสิทธิ์การใช้งานทันทีเมื่อออกจากองค์กรทั้งบุคลากรภายในและภายนอกเป็นระบบอัตโนมัติ
- 2. มีการกำหนดขั้นตอนการปฏิบัติและขั้นตอนในการถอดถอนสิทธิ์การใช้งานทันทีเมื่อออกจากองค์กรเฉพาะบุคลากรภายนอก ส่วนบุคลากรภายในจะต้องได้รับการ

ตรวจสอบในการสิ้นสุดการทำงานก่อน

- 3. มีการกำหนดขั้นตอนการปฏิบัติและขั้นตอนในการถอดถอนสิทธิ์การใช้งาน ต่อเมื่อได้รับการแจ้งหรือยืนยันอย่างเป็นทางการเท่านั้น
- 4. ไม่แน่ใจว่าองค์กรมีการกำหนดหรือไม่ จำได้ว่าต้องมีการลงทะเบียนสำหรับผู้ใช้งานใหม่ก่อนกับฝ่ายไอที
- 5. ไม่มีการกำหนดขั้นตอนการปฏิบัติแต่อย่างใด

5.4 องค์มีการกำหนดระดับสิทธิ์การเข้าถึงระบบงาน ระบบปฏิบัติการ ระบบฐานข้อมูล หรือระบบงานอื่นๆ เหมาะสมต่อความจำเป็นของผู้ใช้งานแต่ละตำแหน่งหรือไม่

- 1. มีการกำหนดสิทธิ์ในการเข้าถึงเฉพาะระบบที่เกี่ยวข้องกับบุคคลและส่วนงาน นั้นๆ อย่างเหมาะสมไม่อนุญาตให้บุคคลหรือส่วนงานอื่นที่ไม่เกี่ยวข้องเข้าถึงระบบงานอื่น
- 2. มีการกำหนดสิทธิ์เข้าใช้งานระบบเฉพาะบุคลากรที่เกี่ยวข้องกับงาน หากส่วนงานอื่นหากมีความจำเป็นต้องเข้าใช้งานระบบงานอื่นต้องทำการขออนุญาตผู้บริหารก่อนทุกครั้ง
- 3. กำหนดสิทธิ์เพียงแค่เจ้าหน้าที่ปฏิบัติงานเท่านั้นส่วนผู้บริหารหรือหัวหน้างานสามารถเข้าใช้งานได้ทุกระบบงาน
- 4. ไม่มีการกำหนดสิทธิ์การใช้งานให้ระบบหรือบุคคลแต่อย่างใด
- 5. ไม่แน่ใจว่ามีการกำหนดสิทธิ์การใช้งานหรือไม่ เพราะไม่ทราบข้อมูลอะไรเลย

5.5 องค์กรมีการอบรมให้ความรู้ แนวทางการกำหนดรหัสผ่านเกี่ยวกับการใช้งานด้านเทคโนโลยีสารสนเทศที่ปลอดภัยให้แก่บุคลากรในองค์กรหรือไม่

- 1. มีการอบรมให้ความรู้อย่างสม่ำเสมอโดยวิทยากรที่มีความชำนาญ
- 2. ไม่มีการอบรม มีการประชาสัมพันธ์ประกาศแจ้งเป็นโปสเตอร์แต่ไม่มีการอบรม
- 3. ไม่มีการจัดอบรมในองค์กรแต่มีประชาสัมพันธ์ในกรณีที่องค์กรภายนอกมีการประชุมให้ความรู้ ฟรี
- 4. ไม่มีการอบรมให้ความรู้ แต่หากใครสงสัยสามารถสอบถามที่ได้เจ้าหน้าที่ด้านไอที
- 5. ไม่มีการจัดอบรมให้ความรู้ในเรื่องนี้เลย

5.6 องค์กรมีการกำหนดระยะเวลาสิ้นสุดการใช้งานของระบบงานเมื่อไม่มีกิจกรรมหรือมีการกำหนดระยะเวลาในการเชื่อมต่อระบบงานหรือไม่

- ☐ 1. มีการกำหนดระยะเวลาในการเชื่อมระบบงานเมื่อสิ้นสุดการใช้งานภายในองค์กร
- ☐ 2. มีการกำหนดระยะเวลาเฉพาะส่วนงานภายในองค์กร
- ☐ 3. มีการกำหนดระยะเวลาในการเชื่อมต่อแต่เมื่อมีการตัดระบบก็สามารถเชื่อมต่อได้
- ☐ 4. มีการกำหนดระยะเวลาเฉพาะบุคคลภายนอกเท่านั้นไม่มีการกำหนดระยะเวลาสำหรับบุคลากรภายใน
- ☐ 5. ไม่มีการกำหนดระยะเวลาใดๆ

5.7 องค์กรมีนโยบายหรือข้อกำหนดการตรวจสอบควบคุมการใช้งานโปรแกรมอรรถประโยชน์นอกเหนือจากที่องค์กรกำหนดหรือไม่

- ☐ 1. มีการกำหนดนโยบายตรวจสอบและควบคุมการใช้งานโปรแกรมที่นอกเหนือจากที่องค์กรกำหนดตลอดทุกปีการศึกษา
- ☐ 2. มีการกำหนดนโยบายและควบคุมการใช้งานโปรแกรมที่นอกเหนือจากที่องค์กรกำหนด บ้างนานๆครั้ง
- ☐ 3. มีนโยบายในการตรวจสอบแต่เฉพาะมีเหตุการณ์ที่สุวิสัยที่เกิดขึ้นเท่านั้น
- ☐ 4. ไม่มีการกำหนดนโนบายในการตรวจสอบแต่มีการสุ่มตรวจสอบการใช้งานตามคำสั่งของผู้บริหารเท่านั้น
- ☐ 5. ไม่มีการตรวจสอบและควบคุมการใช้งานแต่อย่างใด

<u>ด้านที่ 6 การควบคุมการเข้ารหัสข้อมูล</u>

6.1 องค์กรมีการกำหนดนโยบายการเข้าใช้งานรหัสข้อมูล และมีการตรวจสอบการใช้งานตามนโยบายหรือไม่

- ☐ 1. มีนโยบายการใช้งาน มีการตรวจสอบการใช้งานตามนโยบาย 1 ครั้ง/เดือน
- ☐ 2. มีนโยบายการใช้งาน มีการตรวจสอบการใช้งานตามนโยบาย 6 ครั้ง/ปี
- ☐ 3. มีนโยบายการใช้งาน มีการตรวจสอบการใช้งานตามนโยบาย 1 ครั้ง/ปี
- ☐ 4. มีการกำหนดนโยบายการใช้งาน แต่ไม่มีนโยบายการตรวจสอบการใช้งาน
- ☐ 5. ไม่มีการกำหนดนโยบายการใช้งาน และการตรวจสอบ

ด้านที่ 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

7.1 องค์กรมีการกำหนดขอบเขตหรือบริเวณโดยรอบทางกายภาพที่ต้องมีการรักษาความมั่นคงปลอดภัยการแบ่งแยกพื้นที่เหมาะสมหรือไม่

- 1. องค์กรมีการกำหนดนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการใดๆ รวมถึงการกำหนดขอบเขตหรือบริเวณโดยรอบทางกายภาพที่ต้องมีการรักษาความมั่นคงเพื่อนำมาใช้ในการป้องกันสารสนเทศจากการคุกคามของบุคคล ภัยธรรมชาติ หรือภัยทางกายภาพอื่นๆ
- 2. องค์กรมีการกำหนดขอบเขตและแบ่งแยกพื้นที่การใช้งานได้อย่างเหมาะสม
- 3 องค์กรมีการกำหนดขอบเขตและแบ่งแยกพื้นที่การใช้งานไม่ค่อยเหมาะสม
- 4. องค์กรไม่มีการกำหนดขอบเขตพื้นที่แต่มีการแยกพื้นที่จัดเก็บบางส่วน
- 5. ไม่มีการกำหนดขอบเขตและแบ่งแยกพื้นที่แต่อย่างใด

7.2 องค์กรมีการควบคุมการเข้าออกของพื้นที่เฉพาะผู้ที่มีสิทธิ์หรือผู้ที่ได้รับอนุญาต และได้มีการจัดทำขั้นตอนปฏิบัติสำหรับเข้าออกศูนย์คอมพิวเตอร์ ศูนย์สารสนเทศ อีกทั้งวิธีการสื่อสารถึงผู้ที่เกี่ยวข้องทราบหรือไม่

- 1. องค์กรมีการควบคุมการเข้าออกพื้นที่และติดประกาศขั้นตอนการปฏิบัติสำหรับการเข้าออกศูนย์สารสนเทศอย่างชัดเจน
- 2. องค์กรมีระบบจัดเก็บหรือบันทึกข้อมูลการเข้าออกศูนย์คอมพิวเตอร์ หรือศูนย์สารสนเทศ ของบุคคลต่างๆ
- 3. องค์กรมีการควบคุมการเข้าออกพื้นที่แต่ไม่มีการกำหนดขั้นตอนการการเข้า-ออก
- 4. องค์กรไม่มีการควบคุมการเข้าออกพื้นที่ตามการประกาศประชาสัมพันธ์
- 5. ไม่มีการควบคุมการเข้าออกหรือกำหนดแนวปฏิบัติแต่อย่างใด

7.3 องค์กรมีการออกแบบการรักษาความมั่นคงปลอดภัย ทางกายภาพของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวก หน่วยงานสารสนเทศ และศูนย์คอมพิวเตอร์ หรือไม่ เช่น มี Access Control หรือกล้องวงจรปิด เป็นต้น

- 1. องค์กรมีการแบ่งพื้นที่การรักษาความปลอดภัย พร้อมทั้งติดตั้งระบบการรักษาความปลอดภัย และอุปกรณ์อำนวยความสะดวกได้อย่างเหมาะสม

- 2. องค์กรมีการแบ่งพื้นที่การรักษาความปลอดภัย พร้อมทั้งติดตั้งระบบการรักษาความปลอดภัย และอุปกรณ์อำนวยความสะดวกแต่ไม่มีการตรวจสภาพความพร้อมการใช้งานตามระยะเวลาที่กำหนด
- 3. องค์กรมีการติดตั้งระบบรักษาความปลอดภัยแต่ยังไม่ครอบคลุมทุกพื้นที่ในองค์กร
- 4. องค์กรมีการติดตั้งระบบรักษาความปลอดภัยแต่ไม่ค่อยเหมาะสมในพื้นที่เท่าที่ควร
- 5. ไม่มีการติดตั้งระบบรักษาความปลอดภัยแต่อย่างใด

7.4 องค์กรมีการมี การป้องกันภัยทางธรรมชาติการโจมตีหรือการบุกรุกจากภายนอก อุบัติเหตุที่เหมาะสมและมีการตรวจสอบการใช้งานอย่างสม่ำเสมอหรือไม่ เช่น มีการติดตั้ง Fire Alarm, Air Condition, Smoke Detector, เครื่องตรวจวัดความชื้น, ถังดับเพลิง เป็นต้น

- 1. องค์กรมีการติดตั้งอุปกรณ์ป้องกันภัยอย่างเพียงพอและเหมาะสม รวมทั้งมีการกำหนดระยะเวลาในตรวจสอบอุปกรณ์อย่างสม่ำเสมอ
- 2. องค์กรมีการติดตั้งอุปกรณ์ป้องกันภัยแต่ยังไม่เพียงพอกับการใช้งาน
- 3. องค์กรมีการติดตั้งอุปกรณ์ป้องกันภัยที่เพียงพอ ในพื้นที่ที่เหมาะสม แต่การตรวจสอบอุปกรณ์ป้องกันภัยไม่สอดคล้องกับระยะเวลาตามข้อแนะนำการใช้อุปกรณ์ตามที่กำหนด
- 4. องค์กรมีการติดตั้งอุปกรณ์ป้องกันภัยที่เพียงพอ แต่ไม่มีการตรวจสอบตามรอบระยะเวลาการใช้งาน
- 5. มีการอุปกรณ์ป้องกันภัยที่ไม่เพียงพอและติดตั้งในพื้นที่ที่ไม่เหมาะสม และไม่มีการกำหนดระยะเวลาการใช้งาน

7.5 องค์กรมีการจัดวางอุปกรณ์สารสนเทศได้อย่างเหมาะสม ปลอดภัย และกำหนดให้ผู้มีสิทธิ์เท่านั้นที่สามารถเข้าถึงอุปกรณ์ได้อย่างเหมาะสมหรือไม่

- 1. องค์กรมีการจัดวางอุปกรณ์สารสนเทศและมีการกำหนดสิทธิ์ผู้ที่สามารถเข้าถึงอุปกรณ์นั้นๆ ได้อย่างเหมาะสม
- 2. องค์กรมีการจัดวางอุปกรณ์สารสนเทศอย่างเหมาะสม แต่ไม่มีการกำหนดสิทธิ์ผู้ที่สามารถเข้าถึงอุปกรณ์นั้นๆ
- 3. องค์กรมีการจัดวางอุปกรณ์สารสนเทศแต่ยังไม่มีความเหมาะสมเท่าที่ควร

- 4. องค์กรมีการจัดวางอุปกรณ์สารสนเทศแต่ยังไม่มีผู้รับผิดชอบโดยตรงแต่ให้ทุกคนในองค์กรร่วมกันรับผิดชอบ ดูแลรักษาอุปกรณ์
- 5. มีการจัดวางอุปกรณ์ที่ไม่เหมาะสมและไม่ปลอดภัยอีกทั้งยังไม่มีผู้ดูแลชัดเจน

7.6 องค์กรมีการป้องกันการหยุดชะงักของอุปกรณ์ขณะทำงาน เช่น มีการติดตั้ง UPS สำรองไฟ ระบบควบคุมอุณหภูมิ และเครื่องกำเนิดไฟฟ้า เป็นต้น ในแต่ละส่วนงานหรือไม่

- 1. องค์กรมีการติดตั้งอุปกรณ์สำรองเพื่อให้การทำงานได้อย่างต่อเนื่องทุกส่วนงาน
- 2. องค์กรมีการติดตั้งอุปกรณ์สำรองเพื่อให้การทำงานได้อย่างต่อเนื่องบางส่วนงานที่สำคัญเท่านั้น
- 3. องค์กรมีการติดตั้งอุปกรณ์สำรองเพื่อให้การทำงานได้อย่างต่อเนื่องบางส่วนงานที่สำคัญเท่านั้นแต่ยังไม่ได้รับการดูแลรักษาให้ใช้งานได้อย่างต่อเนื่อง
- 4. องค์กรมีการติดตั้งอุปกรณ์สำรองเพื่อให้การทำงานได้อย่างต่อเนื่องบางส่วนงานที่สำคัญเท่านั้นแต่ไม่ได้มีการดูแลรักษา
- 5. องค์กรไม่มีการจัดเตรียมอุปกรณ์ไว้ใช้ในการสำรอง

7.7 องค์กรมีการจัด ทำ Label และ จัดระเบียบ สายไฟ สายสื่อสาร และสายเคเบิ้ล เพื่อไม่ก่อให้เกิดการขัดขวางการทำงาน ป้องกันการแทรกแซงสัญญาณหรือการทำให้เสียหายหรือไม่

- 1. องค์กรมีการจัดทำ Label และการมีตรวจประเมินความพร้อม และจัดการป้องกันไม่ให้เกิดความเสียหายของสายไฟสายสื่อสาร และสายเคเบิ้ลทุก 6 เดือน
- 2. องค์กรมีการจัดทำ Label และการมีตรวจประเมินความพร้อม และจัดการป้องกันไม่ให้เกิดความเสียหายของสายไฟสายสื่อสาร และสายเคเบิ้ลทุก 1 ปี
- 3. องค์กรไม่มีการจัด Label แต่มีการตรวจประเมินสายไฟ สายสัญญาณ สายเคเบิ้ล
- 4. องค์กรมีการจัดทำ Label แต่มีการจัดระเบียบสายไฟ สายสัญญาณ สายเคเบิ้ล ตั้งแต่เริ่มติดตั้งแต่ไม่มีการตรวจสอบเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น
- 5. องค์กรไม่มีการดำเนินการใดที่เป็นการป้องกันไม่ให้เกิดความเสียหาย

7.8 องค์กรมีการกำหนดขั้นตอนการปฏิบัติ รักษาความปลอดภัยทรัพย์สินที่นำไปใช้งานนอกองค์กรหรือไม่

- 1. องค์กรมีข้อกำหนด นโยบายการปฏิบัติในการรักษาความปลอดภัยของทรัพย์สินที่ถูกนำออกไปใช้ภายนอกอย่างชัดเจนและมีการตรวจสอบการใช้งานทุกครั้งตามรอบระยะเวลา
- 2. องค์กรมีข้อกำหนด นโยบายการปฏิบัติในการรักษาความปลอดภัยของทรัพย์สินที่ถูกนำออกไปใช้ภายนอกอย่างชัดเจน แต่ไม่มีการตรวจสอบการใช้งานทุกครั้งตามรอบระยะเวลา
- 3. องค์กรมีไม่มีข้อกำหนดหรือนโยบายแต่มีการตรวจสอบอุปกรณ์การใช้ตามรอบระยะเวลา
- 4. องค์กรไม่มีการกำหนดหรือนโยบายแต่ให้สิทธิ์เฉพาะเจ้าของผู้รับผิดชอบส่วนงานเท่านั้นที่สามารถนำอุปกรณ์ออกไปใช้งานได้
- 5. ไม่มีข้อกำหนดหรือนโยบายการใช้งานปุกรณ์ที่ถูกนำไปใช้งานภายนอกแต่อย่างใด

7.9 องค์กรมีการกำหนดมาตรการป้องกันอุปกรณ์อมพิวเตอร์ที่ใช้งานขณะที่ไม่มีผู้ดูแลหรือการใช้งาน หรือไม่ เช่น มีการปิดหน้าจอและกำหนดการเข้ารหัสในการใช้งาน เป็นต้น

- 1. องค์กรมีการกำหนดให้บุคลากรทุกคนที่ใช้อุปกรณ์สารสนเทศในองค์กรตั้งรหัสล็อคหน้าจออัตโนมัติเมื่อหน้าจอไม่มีการทำงาน
- 2. องค์กรมีการกำหนดให้บุคลากรทุกคนที่ใช้อุปกรณ์สารสนเทศในองค์กรตั้งรหัสล็อคหน้าจออัตโนมัติเมื่อหน้าจอไม่มีการทำงาน แต่ไม่มีการปรับปรุงข้อมูลรหัสล็อคหน้าจอให้เป็นปัจจุบัน หรือตรวจสอบ User ว่าเป็นเจ้าของรหัสตัวจริงหรือไม่
- 3. องค์กรมีข้อกำหนดในการตั้งรหัสแต่ไม่มีการดำเนินการหรือบทลงโทษสำหรับผู้ไม่กระทำแต่อย่างใด
- 4. องค์กรไม่มีการออกมาตรการหรือกำหนดขั้นตอนแต่อย่างใด แต่ให้ขึ้นอยู่กับผู้ใช้งานเท่านั้น
- 5. องค์กรไม่มีการกำหนดมาตรการแต่อย่างใด

ด้านที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ

8.1 องค์กรมีการกำหนดขั้นตอนปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรและเป็นปัจจุบันหรือไม่ เช่น ขั้นตอนการปฏิบัติงานในศูนย์คอมพิวเตอร์การสำรองข้อมูล การนำเข้าข้อมูลระบบในงาน การกู้คืนระบบ เป็นต้น

- ☐ 1. มีการกำหนดขั้นตอนการทำงานเป็นลายลักษณ์อักษร ได้รับอนุมัติจากผู้บริหาร พร้อมทั้งประชุมชี้แจงทำความเข้าใจกับทุกส่วนงานในภาพรวม
- ☐ 2. มีการกำหนดขั้นตอนการทำงานเป็นลายลักษณ์อักษรและอนุมัติจากผู้บริหาร พร้อมทั้งการประชุมชี้แจงทำความเข้าใจเฉพาะงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
- ☐ 3. มีการกำหนดขั้นตอนการทำงานเป็นลายลักษณ์อักษรและได้รับการอนุมัติจากผู้บังคับบัญชา แต่ไม่มีการสื่อสารไปยังผู้ที่เกี่ยวข้องโดยตรง
- ☐ 4. มีการกำหนดขั้นตอนการในการทำงานที่เป็นลายลักษณ์อักษรแต่ไม่ได้เป็นเรื่องเกี่ยวกับระบบเทคโนโลยีสารสนเทศโดยตรงทั้งหมด
- ☐ 5. ไม่มีการกำหนดขั้นตอนในการปฏิบัติงาน

8.2 องค์กรมีการตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ตั้งโต๊ะของบุคลากรในองค์กรหรือไม่ ว่ามีการติดตั้ง Anti-virus และตั้ง Auto Update รวมถึงการสร้างความตระหนักในการจัดการโปรแกรมไม่ประสงค์ดี

- ☐ 1. มีการตรวจสอบทุกๆ สามเดือน เป็นประจำสม่ำเสมอและให้ข้อมูลเพื่อสร้างความตระหนักให้บุคลากรในองค์กร
- ☐ 2. มีการตรวจสอบทุกๆ หกเดือน เป็นประจำสม่ำเสมอและให้ข้อมูลเพื่อสร้างความตระหนักให้บุคลากรในองค์กร
- ☐ 3. มีการตรวจสอบทุกๆปี แต่ไม่มีการให้ข้อมูลความรู้ในการสร้างความตระหนักรู้
- ☐ 4. มีการตรวจทุกครั้งที่มีปัญหาเกิดขึ้นและจะให้ข้อมูลแนะนำในบางกรณี
- ☐ 5. ไม่มีการตรวจสอบและสร้างความตระหนักรู้แต่อย่างใด

8.3 องค์กรมีการกำหนดขั้นตอนการสำรองข้อมูลและรายงานผลการทดสอบข้อมูลที่สำรองต่อผู้บังคับบัญชาอย่างสม่ำเสมอหรือไม่

- 1. มีการกำหนดขั้นตอนการปฏิบัติและรายงานผลการทดสอบตามรอบเวลาที่กำหนดอย่างสม่ำเสมอ
- 2. มีการกำหนดขั้นตอนการปฏิบัติและทดสอบข้อมูล แต่ไม่มีการรายงานผลการทดสอบอย่างสม่ำเสมอ
- 3. มีการกำหนดขั้นตอนการปฏิบัติ แต่ไม่มีการทดสอบและรายงานผลการทดสอบ
- 4. ไม่มีการกำหนดขั้นตอนการปฏิบัติ แต่มีการทดสอบตามที่เห็นสมควรและไม่ได้รายงานผล
- 5. ไม่มีการกำหนดขั้นตอนการปฏิบัติ

8.4 องค์กรมีการกำหนดสิทธิการเข้าถึงอุปกรณ์บันทึกล็อคเฉพาะผู้มีสิทธิ์หรือไม่

- 1. องค์กรมีการกำหนดระดับสิทธิ์ในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ
- 2. องค์กรมีการกำหนดสิทธิ์ในการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- 3. องค์กรมีการกำหนดสิทธิ์ในการเข้าถึงเฉพาะบุคลากรในองค์กรเท่านั้น
- 4. องค์กรไม่มีระบบบันทึกล็อก
- 5. องค์กรไม่มีการกำหนดสิทธิ์ในการเข้าถึงใครก็สามารถเข้าถึงได้

8.5 องค์กรมีการตั้งเวลาของระบบที่สำคัญทั้งหมดในองค์กรว่าถูกต้อง ตรงกันกับอุปกรณ์เทียบเวลาจากแหล่งอ้างอิง NTP Server หรือไม่

- 1. องค์กรมีการตั้งเวลาของระบบที่สำคัญทั้งหมดโดยอ้างเวลา NTP Server
- 2. องค์กรมีการตั้งเวลาของระบบบางระบบโดยอ้างเวลา NTP Server
- 3. องค์กรมีการตั้งเวลาของระบบแต่ไม่ได้อ้างอิงจาก NTP Server
- 4. องค์กรไม่มีระบบที่สำคัญมากจึงไม่ได้อ้างอิงเวลาจาก NTP Server
- 5. องค์กรไม่มีการตั้งเวลาระบบที่สำคัญ

8.6 องค์กรมีการติดตาม เฝ้าระวัง และประเมินความเสี่ยงช่องโหว่ที่เกิดขึ้น และมีมาตรการจัดการช่องโหว่ที่เกิดขึ้นอย่างเหมาะสม ทันเวลาหรือไม่

- 1. องค์กรมีการติดตาม เฝ้าระวัง และประเมินความเสี่ยงที่อาจเกิดขึ้นจากช่องโหว่อย่างสม่ำเสมอ รวมถึงมีการวางแผนการจัดการอย่างเหมาะสม
- 2. องค์กรมีการติดตาม เฝ้าระวัง และประเมินความเสี่ยงที่อาจเกิดขึ้นจากช่องโหว่ แต่ไม่มีการทบทวนมาตรการให้เป็นปัจจุบัน
- 3. องค์กรมีการติดตาม เฝ้าระวัง และประเมินความเสี่ยงที่อาจเกิดขึ้นจากช่องโหว่แต่มาตรการยังไม่ครอบคลุมความเสี่ยงที่อาจเกิดขึ้น
- 4. องค์กรไม่ได้มีการติดตามเฝ้าระวังอย่างสม่ำเสมอแต่มีมาตรการเตรียมไว้หากเกิดกรณีฉุกเฉินขึ้น
- 5. ไม่มีการเฝ้าติดตามและมาตรการในการป้องกันหรือจัดการ

8.7 องค์กรมีการตรวจสอบควบคุมการติดตั้งซอฟต์แวร์ ว่ามีความเหมาะสมและเป็นปัจจุบันหรือไม่

- 1. องค์กรมีการตรวจสอบ ควบคุมการติดตั้งซอฟต์แวร์เป็นประจำสม่ำเสมอและเหมาะสมเป็นปัจจุบัน
- 2. องค์กรมีการตรวจสอบ ควบคุมการติดตั้งซอฟต์แวร์ แต่ไม่มีการปรับปรุงซอฟต์แวร์อย่างสม่ำเสมอ
- 3. องค์กรมีมาตรการควบคุมแต่ไม่มีการตรวจสอบการติดตั้งซอฟต์แวร์อย่างสม่ำเสมอ
- 4. องค์กรมีมาตรการควบคุมแต่ไม่มีการตรวจสอบการติดตั้งซอฟต์แวร์เลย
- 5. องค์กรไม่มีมาตรการควบคุม ตรวจสอบ การติดตั้งซอฟต์แวร์เลย

ด้านที่ 9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์

9.1 องค์กรมีการบริหารจัดการควบคุมเครือข่าย โดยแบ่งแยกโซนเครือข่าย และแบ่งแยก VLAN กลุ่มผู้ใช้งานหรือไม่

- 1. องค์กรมีการจัดการควบคุมแบ่งแยกโซนเครือข่ายและแบ่งแยก VLAN กลุ่มผู้ใช้งาน
- 2. องค์กรมีการจัดการควบคุมแบ่งแยกโซนเครือข่ายและแบ่งแยก VLAN กลุ่มผู้ใช้งาน แต่ยังไม่มีการควบคุมการเข้าถึงทรัพยากรจากบุคคลภายนอก

- 3. องค์กรมีการจัดการควบคุมแบ่งแยกโซนเครือข่ายแต่ยังไม่มีการแบ่งแยก VLAN กลุ่มผู้ใช้งาน
- 4. องค์กรมีการแบ่งแยก VLAN กลุ่มผู้ใช้งาน แต่ไม่มีการจัดการควบคุมแบ่งแยกโซนเครือข่าย
- 5. องค์กรไม่มีการจัดการควบคุมแบ่งโซน เครือข่ายระหว่างกลุ่มผู้ใช้งาน

9.2 องค์กรมีการกำหนดระดับของข้อตกลงในการให้บริการเครือข่ายไว้อย่างเหมาะสม ทั้งการให้บริการภายในและภายนอกองค์กรหรือไม่

- 1. องค์กรมีการกำหนดข้อตกลงระดับการให้บริการไว้อย่างเหมาะสม
- 2. องค์กรมีการกำหนดข้อตกลงแต่ยังไม่ครอบคลุมเครือข่ายและประเภทผู้ใช้งาน
- 3. องค์กรมีการกำหนดข้อตกลงแต่ไม่ชัดเจนกับผู้ให้บริการและประเภทผู้ใช้งาน
- 4. องค์กรมีการกำหนดข้อตกลงแต่ไม่มีการทบทวนข้อตกลงให้เป็นปัจจุบันหรือสอดคล้องกับสภาพการณ์
- 5. องค์กรไม่มีการกำหนดข้อตกลงแต่อย่างใด

9.3 องค์กรมีการกำหนดนโยบาย ขั้นตอนการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานภายนอกตลอดจนการรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูลสารสนเทศขององค์กรกับหน่วยงานภายนอกหรือไม่

- 1. องค์กรมีการกำหนดเป็นนโยบายและข้อปฏิบัติในการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานภายนอกไว้อย่างครอบคลุมและมีความปลอดภัย
- 2. องค์กรมีการกำหนดขั้นตอนการปฏิบัติในการแลกเปลี่ยนสารสนเทศและการรักษาความลับระหว่างองค์กรภายในเท่านั้นยังไม่มีการกำหนดระหว่างหน่วยงานภายนอก
- 3. องค์กรมีการกำหนดนโยบาย ขั้นตอนการแลกเปลี่ยนสารสนเทศที่ปลอดภัยแต่ไม่มีข้อตกลงเกี่ยวกับการไม่เปิดเผยข้อมูลขององค์กร
- 4. องค์กรไม่มีการกำหนดกระบวนการแลกเปลี่ยนข้อมูลสารสนเทศให้ชัดเจนตั้งแต่ขั้นตอนการเตรียมการ การเริ่มดำเนินการ ระหว่างดำเนินการ และสิ้นสุดการดำเนินการ
- 5. องค์กรไม่มีการกำหนดเป็นนโยบายหรือข้อตกลงใดๆ

ด้านที่ 10 การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ

10.1 **องค์กรมีกระบวนการป้องกันข้อมูลสารสนเทศจากการถูกเปิดเผยหรือเปลี่ยนแปลงแก้ไขข้อมูลโดยผู้ที่ไม่มีสิทธิ รวมถึงมีการวิเคราะห์ช่องโหว่หรือการทดสอบเจาะระบบการส่งข้อมูลผ่านเครือข่ายสาธารณะหรือไม่**

- 1. องค์กรมีกระบวนการในการป้องกันการเข้าถึงข้อมูลจากการส่งผ่านเครือข่ายสาธารณะโดยผู้ที่ไม่มีสิทธิ์
- 2. องค์กรมีกระบวนการในการป้องกันแต่ไม่มีการทดสอบเจาะระบบที่มีการส่งข้อมูล
- 3. องค์กรมีกระบวนการในการป้องกันเฉพาะเครือข่ายภายใน ส่วนการป้องกันจากเครือข่ายภายนอกยังไม่ครอบคลุมและยังไม่เคยมีการทดสอบเจาะระบบแต่อย่างใด
- 4. องค์กรมีกระบวนการในการป้องกันเฉพาะเครือข่ายภายใน แต่ยังไม่เคยมีการทดสอบเจาะระบบแต่อย่างใด
- 5. องค์กรไม่มีกระบวนการจัดการใดๆ เลย

10.2 **องค์กรมีกระบวนการป้องกันข้อมูลสารสนเทศบนธุรกรรมออนไลน์จากการรับส่งข้อมูลที่ไม่สมบูรณ์ ผิดเส้นทาง หรือมีการเปลี่ยนแก้ไขจากผู้ที่ไม่มีสิทธิหรือไม่**

- 1. องค์กรมีกระบวนการป้องกันข้อมูลสารสนเทศที่มีความเหมาะสม
- 2. องค์กรมีกระบวนการป้องกันข้อมูลสารสนเทศแต่ไม่มีการสอบทานข้อมูลการรับส่งสารสนเทศที่ไม่สมบูรณ์
- 3. องค์กรไม่มีกระบวนการป้องกันข้อมูลสารสนเทศ แต่มีการการสอบทานข้อมูลการรับส่งสารสนเทศที่ไม่สมบูรณ์เป็นบางครั้ง
- 4. องค์กรไม่มีกระบวนการจัดการป้องกันข้อมูลสารสนเทศจะแก้ไขก็ต่อเมื่อมีเหตุการณ์ฉุกเฉิน
- 5. องค์กรไม่มีกระบวนการจัดการป้องกันข้อมูลสารสนเทศ

10.3 **องค์กรมีการกำหนดข้อตกลงในการพัฒนาระบบให้มีความมั่นคงปลอดภัย และมีการตรวจสอบว่ามีการปฏิบัติตามข้อตกลงหรือไม่**

- 1. องค์กรมีการกำหนดข้อตกลงในการพัฒนาระบบให้มีความมั่นคงปลอดภัยและมีการตรวจสอบการปฏิบัติอย่างสม่ำเสมอ

- 2. องค์กรมีการกำหนดข้อตกลงในการพัฒนาระบบให้มีความมั่นคงปลอดภัยแต่ไม่ได้มีการตรวจสอบการปฏิบัติตามข้อตกลงทุกครั้ง
- 3. องค์กรมีการกำหนดข้อตกลงในการพัฒนาระบบให้มีความมั่นคงปลอดภัยแต่ไม่เหมาะสมต่อการนำไปปฏิบัติ
- 4. องค์กรไม่มีการกำหนดข้อตกลงในการพัฒนาระบบให้มีความมั่นคงปลอดภัยนอกจากปฏิบัติตามคำสั่งของผู้บังคับบัญชา
- 5. องค์กรไม่มีการกำหนดข้อตกลงในการพัฒนาระบบให้มีความมั่นคงปลอดภัยและไม่มีการตรวจสอบการปฏิบัติตามข้อตกลง

10.4 องค์กรมีแนวทางการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ รวมถึงมีการทดสอบหลังการเปลี่ยนแปลง โดยได้รับการอนุมัติให้มีการประเมินผลกระทบจากผู้มีอำนาจและมีการรายงานผลทุกครั้งหรือไม่

- 1. องค์กรมีการกำหนดแนวทางการควบคุม ทดสอบ ประเมินผล และรายงานผลระบบทุกครั้งที่มีการเปลี่ยนแปลงโดยได้รับการอนุมัติจากผู้บังคับบัญชาทุกครั้ง
- 2. องค์กรมีการกำหนดแนวทางการควบคุม ทดสอบ ประเมินผลระบบที่มีการเปลี่ยนแปลง แต่มีการรายงานผลเป็นบางครั้งที่มีการแก้ไข
- 3. องค์กรมีการกำหนดแนวทางการควบคุม ทดสอบ ประเมินผลระบบที่มีการเปลี่ยนแปลงแต่ไม่มีการรายงานผลเมื่อมีการแก้ไข
- 4. องค์กรมีการกำหนดแนวทางการควบคุม ประเมินผลในการเปลี่ยนแปลงแก้ไขระบบทุกครั้งแต่ไม่มีการทดสอบหลังการเปลี่ยนแปลง
- 5. องค์กรไม่มีการกำหนดแนวทางการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ

10.5 องค์กรมีการกำหนดหลักวิศวกรรมระบบให้มีความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษรและเป็นปัจจุบันหรือไม่

- 1. องค์กรมีการกำหนดหลักวิศวกรรมระบบที่มีความมั่นคงปลอดภัยเป็นลายลักษณ์อักษร
- 2. องค์กรมีการกำหนดหลักวิศวกรรมระบบที่มีความมั่นคงปลอดภัยเป็นลายลักษณ์อักษร แต่ไม่เป็นปัจจุบัน
- 3. องค์กรมีการกำหนดหลักวิศวกรรมระบบที่มีความมั่นคงปลอดภัยแต่ไม่เป็น

ลายลักษณ์อักษร

- 4. องค์กรมีการกำหนดหลักวิศวกรรมระบบแต่ไม่มั่นใจว่าจะมีความมั่นคงปลอดภัย
- 5. องค์กรไม่มีการกำหนดหลักวิศวกรรมระบบที่มีความมั่นคงปลอดภัยเป็นลายลักษณ์อักษร

ด้านที่ 11 การควบคุมดูแลผู้ให้บริการภายนอก

11.1 องค์กรมีแนวทางปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศระหว่างองค์กรกับผู้ให้บริการภายนอกหรือไม่ เช่น การกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก เป็นต้น

- 1. องค์กรมีแนวทางปฏิบัติงานเพื่อความมั่นคงปลอดภัยร่วมกับผู้ให้บริการภายนอกอย่างชัดเจนเหมาะสม
- 2. องค์กรมีแนวทางปฏิบัติงานเพื่อความมั่นคงปลอดภัยร่วมกับผู้ให้บริการแต่ไม่ได้มีการทบทวนให้เป็นปัจจุบันสอดคล้องกับสถานการณ์ที่เปลี่ยนไป
- 3. องค์กรมีแนวทางปฏิบัติงานร่วมกับผู้ให้บริการภายนอกแต่ยังไม่ครอบคลุมด้านความมั่นคงปลอดภัย
- 4. องค์กรมีแนวทางปฏิบัติงานร่วมกับหน่วยงานภายนอกที่ไม่ชัดเจนด้านความมั่นคงปลอดภัย
- 5. องค์กรไม่มีแนวทางปฏิบัติงานเพื่อความมั่นคงปลอดภัยร่วมกับผู้ให้บริการภายนอก

11.2 องค์กรมีการทำสัญญาจ้างกับผู้ให้บริการภายนอก โดยมีข้อกำหนดในการควบคุมการดำเนินงานของผู้ให้บริการภายนอกและผู้ที่เกี่ยวข้องต้องปฏิบัติตามข้อกำหนดขององค์กรหรือไม่

- 1. องค์กรมีการทำสัญญาจ้างกับผู้ให้บริการภายนอก โดยมีข้อกำหนดควบคุมอย่างชัดเจน
- 2. องค์กรมีการทำสัญญาจ้างกับผู้ให้บริการภายนอก แต่ไม่มีการตั้งข้อกำหนดถึงแนวทางการปฏิบัติที่ชัดเจน
- 3. องค์กรมีการทำสัญญาจ้างกับผู้ให้บริการภายนอก แต่ผู้ให้บริการไม่ค่อยปฏิบัติตามสัญญา
- 4. องค์กรมีการทำสัญญาจ้างกับผู้ให้บริการภายนอกแต่ไม่มีการตั้งข้อกำหนด

 5. องค์กรไม่มีการทำสัญญาจ้างกับผู้ให้บริการภายนอกกับองค์กร

11.3 องค์กรมีการติดตามและทบทวนการให้บริการของผู้ให้บริการภายนอก โดยมีการประเมินผลการให้บริการและรายงานแก่หัวหน้าหรือผู้บังคับบัญชาหรือไม่

 1. องค์กรมีการติดตาม ทบทวนการให้บริการ ประเมินผลการบริการ และรายงานผลต่อผู้บังคับบัญชาให้ทราบอย่างสม่ำเสมอ
 2. องค์กรมีการติดตาม ทบทวนการให้บริการ ประเมินผลการบริการ และรายงานผลต่อผู้บังคับบัญชาให้ทราบเป็นบางครั้ง
 3. องค์กรมีการติดตาม ทบทวนการให้บริการ และประเมินผลการบริการ แต่ไม่มีการรายงานต่อผู้บังคับบัญชาให้ทราบ
 4. องค์กรไม่มีการติดตาม ทบทวนการให้บริการ ประเมินผลการบริการ แต่มีการรายงานผลการดำเนินการโดยทั่วไปต่อผู้บังคับบัญชาให้ทราบตามรอบการใช้บริการ
 5. องค์กรไม่มีการติดตาม ทบทวน หรือประเมินผล รายงานผลให้ผู้บังคับบัญชาทราบแต่อย่างใด

<u>ด้านที่ 12 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ</u>

12.1 องค์กรมีการกำหนดขั้นตอนการรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมหรือไม่

 1. องค์กรมีการกำหนดขั้นตอนการรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและมีเนื้อหาการรายงานเหมาะสม
 2. องค์กรมีการกำหนดขั้นตอนการรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศแต่มีเนื้อหาการรายงานที่ไม่เหมาะสม ไม่สอดคล้องกับเหตุการณ์
 3. องค์กรมีการกำหนดขั้นตอนการรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศแต่มีการรายงานเป็นบางครั้ง
 4. องค์กรไม่มีการกำหนดขั้นตอนการรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศแต่มีการรายงานกรณีมีเหตุเกิดขึ้นเท่านั้น
 5. องค์กรไม่มีการกำหนดขั้นตอนการรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

12.2 องค์กรมีการกำหนดเกณฑ์ประเมินสถานการณ์ความมั่นคงปลอดภัยจากเหตุการณ์ที่ ไม่พึงประสงค์และวิธีแก้ไขเหตุขัดข้องหรือไม่

- ☐ 1. องค์กรมีการกำหนดเกณฑ์ประเมินสถานการณ์ความมั่นคงปลอดภัยและข้อปฏิบัติเมื่อเกิดเหตุขัดข้องไว้
- ☐ 2. องค์กรมีการกำหนดเกณฑ์ประเมินสถานการณ์ความมั่นคงปลอดภัยไว้แต่ไม่ได้กำหนดวิธีปฏิบัติเมื่อเกิดเหตุขัดข้องไว้
- ☐ 3. องค์กรมีการกำหนดเกณฑ์ประเมินสถานการณ์ความมั่นคงปลอดภัยและวิธีปฏิบัติเมื่อเกิดเหตุขัดข้องไว้แต่ไม่ครอบคลุมทุกรายการเมื่อเกิดที่ไม่พึงประสงค์
- ☐ 4. องค์กรไม่ได้มีการจัดทำเป็นเกณฑ์ประเมินสถานการณ์ความมั่นคงฯ ไว้ มีแต่แนวทางการปฏิบัติเบื้องต้นหากเกิดเหตุขัดข้องที่ไม่เป็นลายลักษณ์อักษรและให้รอคำสั่งของผู้ที่เกี่ยวข้องหรือผู้บริหาร
- ☐ 5. องค์กรไม่มีการกำหนดเกณฑ์การประเมินสถานการณ์ความมั่นคงปลอดภัยและข้อปฏิบัติเมื่อเกิดเหตุขัดข้อง

12.3 องค์กรมีการจัดทำสรุปจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยเพื่อหาแนวทางในการแก้ไขระยะยาวหรือไม่

- ☐ 1. องค์กรมีการจัดทำสรุปจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยที่มีการปรับปรุงเป็นปัจจุบันเพื่อใช้เป็นข้อมูลในการแก้ไขปัญหาระยะยาว
- ☐ 2. องค์กรมีการจัดทำสรุปจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยที่มีการปรับปรุงเป็นข้อมูลบางครั้ง
- ☐ 3. องค์กรมีการจัดทำสรุปจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยที่มีการปรับปรุงเป็นข้อมูลบางครั้ง และไม่นำข้อมูลที่ได้ไปใช้ในการวิเคราะห์เพื่อหาแนวทางแก้ไขในระยะยาว
- ☐ 4. องค์กรไม่มีการจัดทำสรุปจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยแต่ใช้วิธีการแก้ปัญหาเฉพาะหน้าเป็นเหตุการณ์ๆ ไป
- ☐ 5. องค์กรไม่มีการจัดทำสรุปจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัย

12.4 องค์กรมีการระบุ รวบรวม จัดหาและจัดเก็บหลักฐานข้อมูลสารสนเทศ เมื่อเกิดเหตุการณ์ที่มีความเกี่ยวข้องกับการดำเนินการทางกฎหมายหรือไม่

- ☐ 1. องค์กรมีการระบุ รวบรวม จัดหาและจัดเก็บหลักฐานข้อมูลสารสนเทศที่ได้รับการปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ
- ☐ 2. องค์กรมีการระบุ รวบรวม จัดหาและจัดเก็บหลักฐานข้อมูลสารสนเทศที่น้อยมาก และนานๆ ถึงจะมีการจัดเก็บ
- ☐ 3. องค์กรมีการระบุ รวบรวม จัดหาและจัดเก็บหลักฐานข้อมูลสารสนเทศแต่ไม่เป็นระเบียบ ยากต่อการค้นหา หรือนำไปใช้ต่อได้โดยสะดวก
- ☐ 4. องค์กรมีแต่การจัดเก็บหลักฐานข้อมูลสารสนเทศที่มีความเกี่ยวข้องกับการดำเนินการทางกฎหมายเท่านั้น
- ☐ 5. องค์กรไม่มีการระบุ รวบรวม จัดหาและจัดเก็บหลักฐานข้อมูลสารสนเทศ

<u>ด้านที่ 13 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ</u>

13.1 องค์กรมีข้อกำหนดสำหรับความมั่นคงปลอดภัยสารสนเทศและความต่อเนื่องเพื่อบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในสถานการณ์ร้ายแรงหรือไม่ เช่น การวางแผนเตรียมการสภาพความพร้อมใช้ของระบบงานในนโยบาย ว่ามีการประเมินผลกระทบทางธุรกิจกรณีระบบงานหยุดชะงักและกำหนดระดับความสำคัญของระบบงานหรือไม่

- ☐ 1. องค์กรมีการเตรียมความพร้อมของระบบให้สามารถใช้งานได้และมีความมั่นคงปลอดภัยอยู่เสมอ
- ☐ 2. องค์กรมีการเตรียมความพร้อมของระบบให้สามารถใช้งานได้แต่ยังไม่ครอบคลุมความมั่นคงปลอดภัยทั้งหมดในภาพรวม
- ☐ 3. องค์กรมีการเตรียมความพร้อมของระบบให้มีความปลอดภัยแต่เป็นการเตรียมความพร้อมที่ยังไม่ได้มีการปรับปรุงข้อมูลให้เป็นปัจจุบัน
- ☐ 4. องค์กรไม่มีการเตรียมความพร้อมของระบบให้มีความปลอดภัยยกเว้นเป็นบางกรณีหรือระบบงานที่มีความสำคัญ
- ☐ 5. องค์กรไม่มีการเตรียมความพร้อมของระบบให้มีความพร้อมใช้งานและความมั่นคงปลอดภัย

13.2 **องค์กรมีการเตรียมสำรองอุปกรณ์ประมวลผลสารสนเทศไว้อย่างเพียงพอตรงตามความต้องการและมีความพร้อมใช้งาน ได้รับการบำรุงรักษาอย่างเหมาะสม และมีสำรองกรณีชำรุดเสียหายไม่ สามารถซ่อมได้หรือไม่**

- ☐ 1. องค์กรมีการเตรียมสำรองอุปกรณ์ประมวลผลสารสนเทศไว้อย่างเพียงพอและได้รับการดูแลรักษาอย่างดี
- ☐ 2. องค์กรมีการเตรียมสำรองอุปกรณ์ประมวลผลสารสนเทศไว้จำนวนหนึ่งแต่หากเกิดชำรุดหรือต้องการพร้อมๆ กันหลายๆ ครั้งอาจมีไม่เพียงพอ
- ☐ 3. องค์กรมีการเตรียมสำรองอุปกรณ์ประมวลผลสารสนเทศไว้จำนวนหนึ่งแต่ไม่สามารถนำมาใช้งานได้เนื่องจากอุปกรณ์ที่สำรองไว้มีความล้าสมัยและไม่สามารถเชื่อมต่อกับระบบขององค์กรได้
- ☐4. องค์กรไม่มีการเตรียมสำรองอุปกรณ์ประมวลผลสารสนเทศไว้ในสำนักงานแต่มีแผนการดำเนินงานที่รองรับกรณีที่เกิดเหตุการณ์ขึ้น โดยการประสานงานกับหน่วยงานภายนอก
- ☐ 5. องค์กรไม่มีการเตรียมสำรองอุปกรณ์ประมวลผลสารสนเทศแต่อย่างใด

<u>ด้านที่ 14 การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด</u>

14.1 **องค์กรมีการจัดทำรายการข้อกฎหมายด้านความมั่นคงปลอดภัยสารสนเทศรวมถึงข้อกำหนดขององค์กรที่ต้องปฏิบัติไว้เป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบัน อีกทั้งได้มีการเผยแพร่ให้คนในองค์กรทราบอย่างทั่วถึงหรือไม่**

- ☐ 1. องค์กรมีข้อกำหนดและทำรายการข้อกฎหมายด้านความมั่นคงปลอดภัยสารสนเทศที่มีการปรับปรุงให้เป็นปัจจุบันเผยแพร่ในสื่อออนไลน์และที่เป็นลายลักษณ์อักษรให้กับบุคลากรในองค์กรได้รับทราบเสมอ
- ☐ 2. องค์กรมีข้อกำหนดและทำรายการข้อกฎหมายด้านความมั่นคงปลอดภัยสารสนเทศที่มีการปรับปรุงให้เป็นปัจจุบันเผยแพร่ในสื่อออนไลน์และที่เป็นลายลักษณ์อักษรให้กับบุคลากรในองค์กรได้รับทราบเป็นบางครั้ง
- ☐ 3. องค์กรมีข้อกำหนดและทำรายการข้อกฎหมายด้านความมั่นคงปลอดภัยสารสนเทศแต่เป็นข้อมูลที่ไม่มีการปรับปรุงให้เป็นปัจจุบันเผยแพร่ให้คนในองค์กรทราบ

- 4. องค์กรไม่มีข้อกำหนดและทำรายการข้อกฎหมายด้านความมั่นคงปลอดภัยสารสนเทศที่ได้รับการปรับปรุงเพื่อเป็นข้อมูลให้บุคลากรทราบ แต่มีการเผยแพร่ข่าวสารที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศโดยทั่วๆ ไป
- 5. องค์กรไม่มีข้อกำหนดและไม่มีการทำรายการข้อกฎหมายด้านความมั่นคงปลอดภัยสารสนเทศที่เผยแพร่ให้บุคลากรในองค์กรทราบเลย

14.2 องค์กรมีการจัดทำขั้นตอนการจัดการลิขสิทธิ์ซอฟต์แวร์ และมีการบริหารจัดการลิขสิทธิ์ซอฟต์แวร์ อย่างเหมาะสมหรือไม่

- 1. องค์กรมีระเบียบการปฏิบัติงานเกี่ยวกับลิขสิทธิ์ซอฟต์แวร์ที่ใช้งานในองค์กรได้อย่างถูกต้องเหมาะสม
- 2. องค์กรมีระเบียบการปฏิบัติงานเกี่ยวกับลิขสิทธิ์ซอฟต์แวร์ที่ใช้งานในองค์กรแต่ไม่ถูกต้อง
- 3. องค์กรมีระเบียบการปฏิบัติงานเกี่ยวกับลิขสิทธิ์ซอฟต์แวร์ที่ใช้งานในองค์กรแต่ไม่ถูกต้องและเหมาะสมครบทุกส่วนงาน
- 4. บุคลากรใช้งานซอฟต์แวร์ โดยไม่มีระเบียบการปฏิบัติงานเกี่ยวกับลิขสิทธิ์ซอฟต์แวร์มารองรับ
- 5. องค์กรไม่มีระเบียบการปฏิบัติงานเกี่ยวกับลิขสิทธิ์ ซอฟต์แวร์ที่ใช้งานในองค์กร

14.3. องค์กรมีการระบุระดับชั้นความลับของข้อมูล การทำป้ายแสดงระดับชั้นความลับและการจัดการสารสนเทศตามนโยบายองค์กรหรือไม่

- 1. องค์กรมีการระบุระดับชั้นความลับของข้อมูล การทำป้ายแสดงระดับชั้นความลับและมีการจัดการสารสนเทศในนโยบายองค์กร
- 2. องค์กรมีการระบุระดับชั้นความลับของข้อมูล แต่ไม่ได้ติดป้ายแสดงระดับชั้นความลับและไม่มีการจัดการสารสนเทศตามนโยบายองค์กร
- 3. องค์กรไม่มีระบุระดับชั้นความลับของข้อมูลเพราะองค์กรไม่มีกำหนดในนโยบาย
- 4. องค์กรไม่มีการระบุระดับชั้นความลับของข้อมูล การทำป้ายแสดงระดับชั้นความลับแต่มีการจัดการสารสนเทศองค์กรในระดับเบื้องต้นเท่านั้น
- 5. องค์กรไม่มีการจัดระดับชั้นความลับของข้อมูลป้ายแสดงระดับชั้นความลับและไม่มีการจัดการสารสนเทศองค์กร

14.4 องค์กรมีการทบทวนการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศโดยผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกเป็นประจำตามรอบระยะเวลาที่กำหนดหรือไม่

- 1. องค์กรมีการทบทวนการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศโดยผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกเป็นประจำตามรอบระยะเวลาที่กำหนด
- 2. องค์กรมีการทบทวนการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศโดยผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกเป็นบางครั้งและไม่ตรงตามรอบระยะเวลาที่กำหนด
- 3. องค์กรไม่มีการทบทวนการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศโดยผู้ตรวจสอบภายนอกและไม่มีการกำหนดระยะเวลาในการตรวจสอบ
- 4. องค์กรมีเพียงการตรวจสอบการใช้งานอุปกรณ์จากเจ้าหน้าที่ไอทีในองค์กรในรอบปี
- 5. องค์กรไม่มีการทบทวนการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศ

14.5. องค์กรมีการทบทวนโยบายความมั่นคงปลอดภัยสารสนเทศโดยการอ้างอิงมาตรฐาน ISO 27001 ฉบับปัจจุบันหรือไม่

- 1. องค์กรมีการทบทวนโยบายความมั่นคงปลอดภัยสารสนเทศโดยการอ้างอิงมาตรฐาน ISO 27001 ฉบับปัจจุบัน
- 2. องค์กรมีการทบทวนโยบายความมั่นคงปลอดภัยสารสนเทศแต่ไม่ใช่มาตรฐาน ISO 27001 ฉบับปัจจุบัน
- 3. องค์กรมีการทบทวนโยบายความมั่นคงปลอดภัยสารสนเทศแต่ไม่ใช่มาตรฐาน ISO
- 4. องค์กรเคยมีการมีการทบทวนโยบายความมั่นคงปลอดภัยสารสนเทศแต่ไม่มีการดำเนินการอย่างต่อเนื่องนานหลายปีแล้ว
- 5. องค์กรไม่มีการทบทวนโยบายความมั่นคงปลอดภัยสารสนเทศกับมาตรฐานใดเลย

แบบสอบถามกลุ่มผู้ใช้งานทั่วไป

แบบสอบถาม การใช้งานสารสนเทศ ของบุคลากรผู้ใช้งานทั่วไปในองค์กร

วัตถุประสงค์ เพื่อสำรวจและเก็บข้อมูลพฤติกรรมการใช้งานเทคโนโลยีสารสนเทศที่ก่อให้เกิดความเสี่ยงไม่ปลอดภัยของข้อมูลในองค์กร นำไปวิเคราะห์พัฒนาระบบประเมินความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศในองค์กรต่อไป

คำอธิบาย : แบบสอบถามแบ่งออกเป็น 2 ตอน ประกอบด้วย ตอนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ตอนที่ 2 เป็นแบบสอบถามที่เกี่ยวข้องกับพฤติกรรมการใช้งานเทคโนโลยีสารสนเทศในองค์กรตามหลักองค์ประกอบมาตรฐานความปลอดภัยพื้นฐาน CIA (Confidentiality, Integrity และ Availability) กรุณาทำเครื่องหมาย √ ลงหน้าข้อคำตอบที่เกี่ยวข้องกับท่านมากที่สุด

ตอนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

1. **ตำแหน่งงานปัจจุบันของคุณคือ**

   ☐ เจ้าหน้าที่ดูแลเกี่ยวกับระบบสารสนเทศองค์กร

   ☐ เจ้าหน้าที่ปฏิบัติงานทั่วไปในองค์กร/หรือสำนักงาน

   ☐ ครู-อาจารย์

   ☐ อื่นๆ ระบุ.....

2. **ปัจจุบันคุณมีอายุ**

   ☐ ระหว่าง 18-29 ปี ☐ ระหว่าง 30-44 ปี ☐ ระหว่าง 45-59 ปี ☐ มากกว่า 59 ปีขึ้นไป

3. **เพศ** ☐ ชาย ☐ หญิง

4. **วุฒิการศึกษาสูงสุด**

   ☐ ต่ำกว่าปริญญาตรี

   ☐ ระดับปริญญาตรี

   ☐ ระดับปริญญาโท

   ☐ ระดับปริญญาเอก

5. อายุการทำงานตำแหน่งปัจจุบันของคุณ

☐ 1-4 ปี ☐ 5-10 ปี ☐ 11-15 ปี ☐ 16-20 ปี ☐ มากกว่า 20 ปีขึ้นไป

6. คุณมีคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ที่สามารถเชื่อมต่ออินเตอร์เน็ตในการทำงานประจำตำแหน่งหรือไม่และเป็นของใคร

☐ มี ของที่ทำงาน ☐ มี ของส่วนตัว ☐ มี ของที่ทำงานและส่วนตั☐ ไม่มี

<u>ตอนที่ 2</u> เป็นแบบสอบถามที่เกี่ยวข้องกับพฤติกรรมการใช้งานเทคโนโลยีสารสนเทศในองค์กรตามหลักองค์ประกอบมาตรฐานความปลอดภัยพื้นฐาน CIA (Confidentiality, Integrity และ Availability)

ด้านที่ 1 Confidentiality : ความลับ การรักษาความลับ โดยส่วนประกอบ 2 ส่วนที่สำคัญที่จะช่วยทำให้ข้อมูลนั้นเป็นความลับได้ก็คือ การกำหนดสิทธิ์ และการพิสูจน์ตัวตน

1.1 องค์กรมีการกำหนดสิทธิ์ผู้ใช้งานเครือข่ายอินเตอร์เน็ต Log in ด้วย ID และ Password ก่อนการใช้งานทุกครั้งหรือไม่

- ☐ 1. มีการกำหนดสิทธิ์เข้างานโดยเครื่องที่สามารถเชื่อมต่ออินเตอร์เน็ตขององค์กรได้ จะต้องได้รับการลงทะเบียนรับ ID และ Password จากเจ้าหน้าที่ก่อน เท่านั้นจึงจะสามารถเข้าใช้งานได้
- ☐ 2. เฉพาะบุคลากรในองค์กรเท่านั้น ที่สามารถใช้งานการเชื่อมต่ออินเตอร์เน็ตขององค์กร และสามารถ Log in เข้าใช้งานได้ด้วย ID และ Password เฉพาะรหัสประจำตัวที่ได้รับการลงทะเบียนแล้วเท่านั้น
- ☐ 3. ทุกคนที่ได้รับสิทธิ์สามารถ Log in เข้าใช้งานได้ ด้วย Password เดียวกันทั้งองค์กร
- ☐ 4. ผู้ที่ได้รับสิทธิ์การเชื่อมต่อฯ สามารถเข้าใช้งานได้ทันทีโดยไม่ต้อง Log in เข้าใช้งาน
- ☐ 5. ไม่มีการกำหนดสิทธิ์การเชื่อมต่อระบบอินเตอร์เน็ตแต่อย่างใด ทุกคนสามารถเข้าใช้งานได้

1.2 องค์กรมีการกำหนดกฎระเบียบเกี่ยวกับการนำอุปกรณ์ส่วนตัว มาเชื่อมต่อเครือข่ายอินเตอร์เน็ตขององค์กรหรือไม่

- ☐ 1. องค์กรมีกฎระเบียบ ไม่อนุญาตให้บุคลากรนำอุปกรณ์ส่วนตัวมาเชื่อมต่อระบบเครือข่ายอินเตอร์เน็ต ยกเว้นอุปกรณ์นั้นได้รับการลงทะเบียนจากเจ้าหน้าที่ขององค์กรเรียบร้อย
- ☐ 2. องค์กรมีกฎระเบียบ ไม่อนุญาตให้บุคลากรนำอุปกรณ์การเชื่อมต่ออินเตอร์เน็ต

ใดๆที่ไม่ใช้อุปกรณ์ของหน่วยงานที่มีการดูแลมาใช้ในการทำงานขององค์กรมาใช้ได้ ยกเว้นอุปกรณ์นั้นได้รับการอนุญาตจากผู้บริหารและได้รับการตรวจสอบจากเจ้าหน้าที่ดูแลระบบแล้วเท่านั้น

☐ 3. องค์กรมีกฎระเบียบ อนุญาตให้เฉพาะบุคลากรในองค์กรที่นำอุปกรณ์มาตรวจสอบและลงทะเบียนกับเจ้าหน้าที่แล้ว เท่านั้น

☐ 4. องค์กรไม่มีกฎระเบียบ บุคลากรในองค์กรสามารถนำอุปกรณ์ส่วนตัวมาใช้งานได้

☐ 5. องค์กรไม่มีกฎระเบียบ ใครก็ได้สามารถนำอุปกรณ์ส่วนตัวมาใช้งานได้ ไม่จำกัด

1.3. อุปกรณ์คอมพิวเตอร์ที่ท่านใช้งานปัจจุบันมีการตั้งรหัสล็อคหน้าจอก่อนการเข้าใช้งานหรือไม่ หากมีท่านมีหลักการตั้งรหัสอย่างไร

☐ 1. มีการตั้งรหัสล็อคหน้าจอไว้ โดยมีตัวอักษร ตัวเลขและอักขระพิเศษรวมกันและทำการเปลี่ยนรหัสทุกๆ 3-6 เดือน

☐ 2. มีการตั้งรหัสล็อคหน้าจอไว้ โดยมีเฉพาะตัวอักษร ตัวเลข โดยยังไม่ได้มีการอัพเดต

☐ 3. มีการตั้งรหัสล็อคหน้าจอ โดยกำหนดการเรียงตัวเลขเรียง 1234 อย่างเดียว

☐ 4. มีการตั้งรหัสล็อคหน้าจอ โดยกำหนดเป็นเบอร์โทรหรือวันเดือนปีเกิดของตนเอง

☐ 5. ไม่มีการตั้งรหัสล็อคหน้าจอแต่อย่างใด สามารถเปิดใช้งานได้เลย

1.4. การเข้าใช้งานเว็บไซต์ต่างๆ ที่มีการ Log in ด้วย ID และ Password หรือต้องทำการยืนยันตัวตนก่อนเข้าใช้งานท่านมีวิธีกำหนดและจัดเก็บรหัสผ่านการเข้าใช้งานอย่างไร

☐ 1. ตั้งรหัสผ่านการใช้งานที่แตกต่างกัน ด้วยการตั้งรหัสที่เราเข้าใจและทราบข้อมูลเพียงผู้เดียวจัดเก็บไว้ในไฟล์เอกสารที่มีการป้องกันอย่างปลอดภัย

☐ 2. ใช้ข้อมูลส่วนตัวในการตั้งรหัสผ่าน แต่มีการตั้งรหัสผ่านที่แตกต่างกัน และหมั่นตรวจสอบการเข้าถึงบัญชีเป็นประจำ

☐ 3. ใช้รูปแบบตัวอักษรหรือตัวเลขที่เป็นที่นิยม “จำรหัสผ่าน” (Remember me) บนเว็บไซต์

☐ 4. ใช้ข้อมูลส่วนตัวในการตั้งรหัสผ่าน และจดรหัสผ่านลงกระดาษหรือในไฟล์เอกสารที่ไม่มีการป้องกันการเข้าถึง

☐ 5. ใช้การเรียงตัวเลขหรืออักษรแบบจำง่ายรหัสเดียวทุกเว็บไซต์ และเปิดเผยรหัสผ่านให้ผู้อื่นรับทราบ จะได้ช่วยจำเวลาเราลืม

1.5. องค์กรท่านมีการกำหนดนโยบายเกี่ยวกับสิทธิในการเข้าถึงข้อมูลเทคโนโลยีสารสนเทศในองค์กรหรือไม่ ท่านปฏิบัติอย่างไรกับนโยบายดังกล่าว

- ☐ 1. มี ปฏิบัติตามอย่างเคร่งครัดทุกข้อ
- ☐ 2. มี ปฏิบัติตามทุกข้อยกเว้นบางข้อที่ไม่สามารถปฏิบัติได้จริงๆ ณ ช่วงเวลานั้นโดยแจ้งให้ผู้บริหารรับทราบถึงเหตุผล
- ☐ 3. มี ปฏิบัติครบทุกข้อเฉพาะครั้งที่มีจะการตรวจสอบภายในองค์กร
- ☐ 4. มี แต่เลือกปฏิบัติเป็นบางข้อที่อยากทำ
- ☐ 5. ไม่มีนโยบาย จึงไม่ได้ปฏิบัติอะไร

1.6. องค์กรของท่านมีการจัดทำแผนพัฒนาระบบสารสนเทศในองค์กรหรือไม่ ใครเป็นผู้ร่วมดำเนินการตามแผนดังกล่าว

- ☐ 1. มีการจัดทำแผนฯ ทั้งระยะสั้นและระยะยาว ทุกคนในองค์กรเป็นผู้ร่วมดำเนินการ
- ☐ 2. มีเฉพาะแผนการพัฒนาฯ ระยะยาว 5 ปี ทุกคนในองค์กรเป็นผู้ร่วมดำเนินการ
- ☐ 3. ไม่มีแผนการพัฒนาฯ แต่มีแผนจัดซื้อประจำปีซึ่งไม่ครอบคลุมถึงการพัฒนาระบบสารสนเทศ ผู้บริหารและเจ้าหน้าที่เกี่ยวข้องเท่านั้นที่เป็นผู้ดำเนินการ
- ☐ 4. ไม่มีแผนการพัฒนาฯ จะดำเนินการต่อเมื่อมีเหตุหรืองบประมาณที่จัดสรรมาเท่านั้น เฉพาะผู้บริหารและเจ้าหน้าที่เกี่ยวข้องเท่านั้น
- ☐ 5. ไม่มีการจัดทำแผนพัฒนาระบบสารสนเทศ

1.7 ท่านคิดว่าการจัดเก็บรหัสผ่านการเข้าใช้งาน (E-mail) ทั้ง ID Password มีความจำเป็นหรือไม่ที่จะจัดเก็บเป็นความลับ และใครบ้างที่สามารถทราบรหัสผ่านการรเข้าใช้งานของท่านได้

- ☐ 1. จำเป็นอย่างยิ่งในการจัดเก็บเป็นความลับ ไม่มีใครทราบรหัสเข้าใช้งาน เนื่องจากได้ทำการเปลี่ยนรหัส ทุก 6 เดือน อย่างสม่ำเสมอ
- ☐ 2. จำเป็นต้องจัดเก็บเป็นความลับ เพื่อนสนิทที่สุดในที่ทำงานเท่านั้นที่จะทราบ
- ☐ 3. จำเป็นต้องจัดเก็บเป็นความลับ แต่หากมีคนมาขอใช้ก็รู้รหัสได้
- ☐ 4. เฉยๆ รู้ก็ได้ ไม่รู้ก็ได้ ใครมาขอใช้ก็ให้รหัสไป
- ☐ 5. ไม่จำเป็น เพื่อนร่วมงานสามารถรับทราบรหัสใช้งานได้

ด้านที่ 2 Integrity : ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความเป็นจริง คือระบบต้องมีกลไกการตรวจสอบสิทธิหรือการได้รับอนุญาตให้ดำเนินการเปลี่ยนแปลงแก้ไขหรือกระทำการใดๆ ต่อข้อมูลนั้น

2.1 ท่านมีความขัดแย้งหรือเคยมีปัญหากับเพื่อนร่วมงานในองค์กรหรือไม่

- ☐ 1. ไม่มี ไม่เคยมีเลย
- ☐ 2. เคยมี แต่นานมาแล้ว ปัจจุบันเข้าใจกันดี
- ☐ 3. มี เวลาที่คุยแล้วความคิดเห็นไม่ตรงกัน
- ☐ 4. มี กับเพื่อนร่วมงานฝ่ายเดียวกัน
- ☐ 5. มีบ่อยเกือบทุกวัน

2.2 คุณมีวิธีการสำรองข้อมูลในงานที่รับผิดชอบอย่างไร

- ☐ 1. สำรองข้อมูลทุกครั้งที่มีการเปลี่ยนแปลงแก้ไขข้อมูล หรืออัพเดต ต่างๆ ทุกเดือน
- ☐ 2. สำรองข้อมูลทุก 3-6 เดือน
- ☐ 3. สำรองบ้างเวลาที่รู้สึกว่าเครื่องจะมีปัญหาและเลือกการสำรองข้อมูล
- ☐ 4. สำรองบ้างนานมาแล้วเมื่อ 2 ปีที่แล้ว
- ☐ 5. ไม่มีการสำรองข้อมูลไว้เลย

2.3 ใครบ้างที่สามารถเข้าใช้งานเครื่องคอมพิวเตอร์ที่ใช้งานประจำของท่านได้

- ☐ 1. ไม่มีใครใช้งานได้เนื่องจากตั้งรหัสผ่านไว้และไม่ได้บอกใคร
- ☐ 2. เฉพาะคนที่ได้รับอนุญาตและทราบรหัสเข้าใช้งานจากเราเท่านั้น
- ☐ 3. เฉพาะผู้บริหาร และเจ้าหน้าที่ไอทีในองค์กรเท่านั้น
- ☐ 4. เพื่อนร่วมงานในองค์กรทุกคนใช้ได้
- ☐ 5. ใครก็ได้ใช้ได้เลย

2.4 ท่านมีการอัพเดตการใช้งานโปรแกรม Anti Virus เครื่องที่ใช้งานประจำหรือไม่ ใครเป็นผู้ดำเนินการให้

- ☐ 1. อัพเดตสม่ำเสมอ โดยเจ้าหน้าที่ดูแลระบบสารสนเทศในองค์กร
- ☐ 2. อัพเดตเองบ้างด้วยตนเอง นานๆครั้ง
- ☐ 3. อัพเดตเฉพาะเวลาที่เครื่องมีปัญหา
- ☐ 4. ไม่มีการอัพเดตเลย เพราะไม่ได้ติดตั้งโปรแกรม Anti Virus
- ☐ 5. ไม่รู้คืออะไร ไม่เคยทำเลย ใช้งานอย่างเดียว

2.5 ทุกครั้งที่เกิดปัญหาจากการใช้งานเทคโนโลยีสารสนเทศในองค์กร ท่านมีวิธีจัดการอย่างไร

- ☐ 1. ปรึกษา ขอคำแนะนำ เจ้าหน้าที่ไอทีในองค์กร แจ้งหัวหน้างานถึงปัญหาและรีบดำเนินการแก้ไข สำรวจความเสียหายของงาน
- ☐ 2. พยายามแก้ไขเองก่อน หากไม่ได้ค่อยตามเจ้าหน้าที่ไอทีมาดูให้
- ☐ 3. เรียกช่างข้างนอกมาดู ช่างที่ไหนว่างก็ให้มาเป็นช่างที่ไม่ได้ทำข้อตกลงกับองค์กร
- ☐ 4. กดไปมั่วๆเดี๋ยวมันก็ดี เพราะเคยทำแล้วมันดีกลับมาใช้งานได้
- ☐ 5. ไม่ทำอะไร หงุดหงิดอารมณ์ไม่ดี รออารมณ์ดีค่อยกลับมาแก้

2.6 องค์กรมีการกำหนดบทลงโทษ ในกรณีที่มีการฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศและได้มีการปฏิบัติตามกฎดังกล่าวหรือไม่

- ☐ 1. มีกำหนดบทลงโทษและให้ทุกคนในองค์กรปฏิบัติอย่างเคร่งครัด
- ☐ 2. มีกำหนดบทลงโทษและมีการปฏิบัติใช้จริงเป็นบางข้อเท่านั้น
- ☐ 3. ไม่มีกำหนดบทลงโทษใดๆ มีแต่แนวปฏิบัติการใช้งานคอมพิวเตอร์ให้ปลอดภัยในองค์กร
- ☐ 4. ไม่มีกำหนดบทลงโทษแต่ทุกครั้งที่เกิดปัญหาจะมีการเรียกสอบสวนเป็นครั้งๆไป
- ☐ 5. องค์กรไม่มีนโยบายใดๆ จึงไม่มีการกำหนดโทษ

ด้านที่ 3 Availability : สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน การตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิเข้าถึงระบบได้เมื่อต้องการ ภัยคุกคามต่อความพร้อมใช้งานของข้อมูล เช่น การโจมตีแบบปฏิเสธการให้บริการต้องใช้มาตรการป้องกัน เช่น การแพตช์ซอฟต์แวร์ปกติ การอัพเกรดระบบการสำรองข้อมูลและการนำกลยุทธ์การกู้คืนระบบ

3.1 ระบบเครือข่ายอินเตอร์เน็ตในองค์กรของท่านสามารถเชื่อมต่อและใช้งานได้ทันทีหรือไม่

- ☐ 1. คนในองค์กรสามารถเข้าใช้งานได้โดยใส่รหัสประจำตัวของแต่บุคคลที่ได้รับ หาบุคคลภายนอกไม่สามารถเชื่อมต่อได้ทันทีเนื่องจากมีการจำกัดสิทธิ์ในการเข้าใช้งาน หากจะใช้ต้องได้รับการลงทะเบียนอุปกรณ์ใช้งานรับ Password ใช้งานกับเจ้าหน้าที่ไอที
- ☐ 2. ไม่สามารถเชื่อมต่อได้ทันที เนื่องจากต้องใส่ Password ก่อน ทั้งคนในองค์กรและบุคคลภายนอกโดยไม่ต้องลงทะเบียนอุปกรณ์การใช้งาน
- ☐ 3. ไม่สามารถเชื่อมต่อได้ทันที ต้องใส่ Password ก่อนทุกครั้งหากใครมี Password ก็

สามารถเชื่อมต่อได้ทั้งหมด

☐ 4. ไม่แน่ใจเพราะปกติก็เข้าใช้งานได้ทันที ส่วนบุคคลภายนอกไม่ทราบ

☐ 5. สามารถเชื่อมต่อเข้าใช้งานได้ทันที ไม่มีการใส่รหัสแต่อย่างใด

3.2 ท่านได้มีการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ที่ใช้งานเป็นประจำสม่ำเสมอหรือไม่

☐ 1. มีการดูแลบำรุงรักษาเป็นประจำอย่างสม่ำเสมอ ทุกๆ 3-6 เดือน หรือทุกครั้งมีการอัพเดตข้อมูล

☐ 2. มีการดูแลทุกๆ 1 ปี

☐ 3. มีการดูแลเฉพาะเวลาที่มีปัญหาเท่านั้น

☐ 4. ดูแลแต่เฉพาะเครื่องส่วนตัว ส่วนเครื่องที่ทำงานไม่ค่อยได้ดูแลเท่าไหร่

☐ 5. ไม่รู้จะดูแลอย่างไร ไม่มีความรู้ด้านนี้ เป็นผู้ใช้งานอย่างเดียว

3.3 ท่านเคยได้รับการอบรมให้ความรู้เกี่ยวการใช้ระบบสารสนเทศที่ปลอดภัยภายในองค์กรหรือไม่

☐ 1. เคย เป็นประจำทุกครั้งที่มีการอัพเดตต่างๆและประจำปีด้วย

☐ 2. ทุกๆสองปี มีการอบรมครั้ง

☐ 3. เคยตั้งแต่ครั้งแรกที่เข้ามาทำงานแล้ว

☐ 4. เคยอบรมแต่ไม่แน่ใจว่าเกี่ยวกับเรื่องนี้โดยตรงรึเปล่า

☐ 5. ไม่เคยเลย

3.4 ทราบหรือไม่ว่า โปรแกรมการใช้งานต่างๆบนอุปกรณ์คอมพิวเตอร์ในสำนักงานของท่าน มีที่มาจากแหล่งใดและเป็นโปรแกรมที่ถูกต้องตามลิขสิทธิ์หรือไม่

☐ 1. ทราบที่มา เนื่องจากองค์กรมีนโยบายการใช้งานโปรแกรมที่เป็นลิขสิทธิ์ของแท้เท่านั้นป้องกันปัญหาที่ตามมาจากการใช้โปรแกรมที่ไม่ถูกต้อง

☐ 2. ทราบที่มา แต่มีบางโปรแกรมที่ไม่ใช่ของแท้ที่ถูกต้องลิขสิทธิ์การใช้งาน

☐ 3. ทราบที่มา ไม่ใช่ของถูกต้องลิขสิทธิ์การใช้งาน ตามที่มี

☐ 4. ไม่ทราบที่มา เจ้าหน้าที่ไอทีนำมาติดตั้งให้ใช้งานได้ก็ถือว่าดี

☐ 5. ไม่ทราบที่มาและไม่ทราบว่าเป็นโปรแกรมลิขสิทธิ์หรือไม่

3.5 คุณมีวิธีปฏิบัติอย่างไร เมื่อมีเหตุให้ต้องลุกออกจากการใช้งานหน้าคอมพิวเตอร์ที่กำลังใช้งานอยู่

☐ 1. กดบันทึกเซฟงานที่กำลังทำ ปิดหน้าต่างที่กำลังใช้งาน ตั้ง Sleep Mode Log หน้าจอเสร็จแล้วไปทำธุระ

☐ 2. กด Minimize หน้าต่างที่กำลังใช้งาน ตั้ง Sleep Mode Log หน้าจอ

☐ 3. กด Minimize Windows ลงและปิดหน้าจอไว้เฉยๆ ไม่ได้ตั้งรหัสล็อคหน้าจอไว้

- [ ] 4. ฝากบอกเพื่อนโต๊ะข้างๆว่าไม่ได้ปิดหน้าจอไว้และจะไปทำธุระก่อนเดี๋ยวมา
- [ ] 5. ไม่ทำอะไรลุกไปทำธุระก่อน เปิดหน้าต่างที่ทำงานทิ้งไว้ เพื่อความสะดวกในการกลับมาทำงานต่อ

3.6 คุณมีหลักหรือแนวทางปฏิบัติในการในการตั้งไอดีและพาสเวิร์ดเข้าใช้งานเว็บไซต์ต่างๆอย่างไร

- [ ] 1. มีตัวอักษรภาษาไทย-อังกฤษ พิมพ์เล็ก-ใหญ่ ตัวเลขและอักขระพิเศษ
- [ ] 2. ใช้เฉพาะตัวเลขและตัวอักษรเท่านั้นในการกำหนดตั้งรหัสผ่าน
- [ ] 3. ใช้ข้อมูลส่วนตัว เช่น วัน เดือน ปีเกิดมาเป็นตัวตั้ง
- [ ] 4. เฉพาะตัวอักษรที่มีความยาว เพียง 6 ตัวเท่านั้น
- [ ] 5. ใช้การเรียงตัวเลข 12345 หรือเรียง 0-9 ง่ายดี

3.7 ความถี่ในการเข้าเปลี่ยนรหัสการใช้งานทั้งเว็บไซค์และอุปกรณ์สารสนเทศต่างๆ ของคุณคือ

- [ ] 1. 3-6 เดือนทั้งเว็บทั้งอุปกรณ์ต่างๆ
- [ ] 2. 1 ปี/ครั้ง เฉพาะอุปกรณ์การใช้งาน
- [ ] 3. นานๆเปลี่ยนทีเมื่อนึกขึ้นได้
- [ ] 4. ไม่เคยเปลี่ยนสักครั้งตั้งแต่การสมัครใช้งานครั้งแรก
- [ ] 5. ไม่มีการตั้งค่าใดๆ จึงไม่มีความจำเป็นต้องเปลี่ยน

3.8 ท่านกำหนดรหัสการเข้าใช้งานเว็บไซต์และอุปกรณ์ต่างๆด้วยรหัสผ่าน เดียวกัน หรือไม่

- [ ] 1. ใช้การกำหนดรหัสผ่าน ที่แตกต่างกัน ไม่ซ้ำกัน ทั้งในอุปกรณ์และเว็บไซต์ต่างๆ
- [ ] 2. ใช้การกำหนดรหัสผ่านที่เหมือนกันเฉพาะเว็บไซต์ประเภทเดียวกัน
- [ ] 3. ใช้การกำหนดรหัสผ่านที่เหมือนกันเฉพาะที่เกี่ยวข้องกับที่ทำงานเท่านั้น
- [ ] 4. ใช้การกำหนดรหัสผ่านอุปกรณ์กับเว็บไซต์รหัสเดียวกัน
- [ ] 5. ใช้การกำหนดเรียงตัวเลข 12345 เหมือนกันทุกการใช้งาน

3.9 ท่านรู้จักระบบปฏิบัติการที่ใช้ในการจัดเก็บข้อมูลทางระบบออนไลน์ อย่างเช่น Cloud หรือ Google Dive หรือไม่

- [ ] 1. รู้จักและใช้งานอยู่และยังมีแพลตฟอร์มอื่นๆอีกให้เลือกใช้งาน
- [ ] 2. รู้จักแต่ไม่ค่อยได้ใช้เท่าไหร่
- [ ] 3. เคยได้ยินแต่ยังไม่เคยใช้งาน
- [ ] 4. ไม่รู้จัก ใช้วิธีเซฟหรือบันทึกในเครื่องหรือแฟลชไดร์อย่างเดียว
- [ ] 5. ไม่รู้จักเลย คืออะไร

3.10 เครื่องคอมพิวเตอร์ที่ท่านใช้งานเคยติดไวรัส หรือ มัลแวร์ หรือไม่

- 1. ไม่เคย เพราะอัพเดตโปรแกรมแอนตี้ไวรัสและมีการตรวจเช็คการใช้งานอย่างสม่ำเสมอ
- 2. เคย แต่นานมาแล้วตอนที่ยังไม่ได้ติดตั้งโปรแกรมสแกนไวรัส
- 3. เคย บ้างส่วนมากมากับแฟลชไดร์ที่มีคนนำมาเสียบที่เครื่อง
- 4. ไม่แน่ใจว่าใช่ไวรัสรึเปล่า ไม่รู้จัก ไม่รู้สาเหตุอยู่ๆข้อมูลก็หาย
- 5. เคยบ่อยมากประจำ

3.11 ท่านอนุญาตให้เพื่อนร่วมงานนำแฟลชไดร์ฟมาบันทึกไฟล์งานหรือข้อมูลต่างๆยังเครื่องที่ท่านใช้งานหรือไม่

- 1. ไม่อนุญาต เพราะกลัวติดไวรัสแล้วข้อมูลในเครื่องหาย
- 2. อนุญาตหากมีความจำเป็น แต่สแกนก่อนทุกครั้ง
- 3. ไม่อนุญาต แต่ ชอบมีเพื่อนร่วมงานแอบมาใช้เครื่อง
- 4. อนุญาตเฉพาะเพื่อนร่วมงานที่สนิทเท่านั้น
- 5. อนุญาตใครอยากใช้ก็เอามาเสียบได้เลย

3.12 ท่านเคยได้รับอีเมล์หรือข้อความที่ไม่ทราบแหล่งที่มาหรือไม่ และท่านปฏิบัติอย่างไรเมื่อได้รับอีเมลนั้น

- 1. ไม่เคยได้รับ เพราะตั้งค่าการรับเข้าอิเมล์ที่ไม่รู้จักไว้
- 2. เคยได้รับ ไม่รู้จักแหล่งที่มาและผู้ส่ง จึงไม่ได้กดเข้าไปดูกลัวเป็นไวรัสจึงลบทิ้ง
- 3. เคยได้รับ เคยลองกดเข้าไปดูและลบทิ้งเพราะไม่รู้จัก
- 4. เคยได้รับ เคยลองกดเข้าไปดูและกรอกข้อมูลบางส่วน
- 5. เคยได้รับ และรีบกดเข้าไปดูไม่ได้ลบทิ้งปล่อยไว้ในอิเมล์

3.13 ท่านทราบหรือไม่ว่าไวรัสหรือมัลแวร์ สามารถทำลายข้อมูลระบบและข้อมูลขององค์กรได้จากเครื่องที่ท่านใช้งาน

- 1. ทราบ และพยายามหลีกเลี่ยงการดาวน์โหลดข้อมูลที่ไม่ทราบแหล่งที่มาและไม่ปล่อยให้มีการนำแฟลชไดร์ฟจากเพื่อนร่วมงานมาใช้ที่เครื่อง
- 2. ทราบ ว่าไวรัสหรือมัลแวร์ สามารถทำลายข้อมูลระบบและข้อมูลขององค์กรได้ แต่ไม่ทราบว่าสามารถทำได้ช่องทางไหนบ้าง
- 3. ทราบแต่ก็ไม่รู้ว่าต้องป้องกันยังไงให้ปลอดภัย
- 4. เหมือนเคยได้ยินแต่ไม่แน่ใจว่าสามารถทำลายข้อมูลได้จริงๆ
- 5. ไม่ทราบ

3.14 ท่านต้องการได้รับการอบรมความปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศเพิ่มเติมหรือไม่ และควรมีช่วงเวลารับการอบรมเท่าไหร่จึงจะเหมาะสมในความคิดของท่าน

- ☐ 1. ต้องการมาก หากมีได้เลยเร็วนี้ก็ดี
- ☐ 2. ต้องการ อย่างน้อยปีละ 1-2 ครั้งกำลังดี
- ☐ 3. มีก็ได้ไม่มีก็ได้ ปีละครั้งก็ได้
- ☐ 4. เฉยๆ แล้วแต่ช่วงเวลา
- ☐ 5. ไม่ต้องการ

ประวัติผู้วิจัย

ชื่อ-สกุล	รสริน ศิริรักษ์
วัน เดือน ปี เกิด	16 สิงหาคม 2530
สถานที่เกิด	อุตรดิตถ์
วุฒิการศึกษา	พ.ศ.2551 ศศ.บ. (นิเทศศาสตร์) มหาวิทยาลัยราชภัฏอุตรดิตถ์,อุตรดิตถ์
ที่อยู่ปัจจุบัน	355 ม.11 ต.บ้านต๋อม อ.เมือง จ.พะเยา
ผลงานตีพิมพ์	รสริน ศิริรักษ์ (อยู่ระหว่างการจัดทำ),