การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

DEVELOPING A CYBERSECURITY CULTURE FRAMEWORK IN ORGANIZATIONS FOR CYBERSECURITY TRANSFORMATION

ฐิติมา ภู่ห้อย

THITIMA PHUHOY

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

มหาวิทยาลัยศรีปทุม

ปีการศึกษา 2564

การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

ฐิติมา ภู่ห้อย

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม
ปีการศึกษา 2564

DEVELOPING A CYBERSECURITY CULTURE FRAMEWORK IN ORGANIZATIONS FOR CYBERSECURITY TRANSFORMATION

THITIMA PHUHOY

A THEMATIC SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

SCHOOL OF INFORMATION TECHNOLOGY

SRIPATUM UNIVERSITY

ACADEMIC YEAR 2021

หัวข้อสารนิพนธ์	การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ DEVELOPING A CYBERSECURITY CULTURE FRAMEWORK IN ORGANIZATIONS FOR CYBERSECURITY TRANSFORMATION
นักศึกษา	ฐิติมา ภู่ห้อย รหัสประจำตัว 64504167
หลักสูตร	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะ	เทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
อาจารย์ที่ปรึกษาสารนิพนธ์	ดร.สุรชัย ทองแก้ว
อาจารย์ที่ปรึกษาสารนิพนธ์ร่วม	ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง

คณะกรรมการสอบสารนิพนธ์

..... ประธานกรรมการ

(รองศาสตราจารย์ ดร.ทศนัย ชุ่มวัฒนะ)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.ปราลี มณีรัตน์)

..... กรรมการ

(ดร.สุรชัย ทองแก้ว)

คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม อนุมัติให้นับสารนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณบดีคณะเทคโนโลยีสารสนเทศ

.....

(ผู้ช่วยศาสตราจารย์ ดร.ธนา สุขวารี)

วันที่ 15 เดือน สิงหาคม พ.ศ. 2565

สารนิพนธ์เรื่อง การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์
คำสำคัญ วัฒนธรรมความมั่นคงปลอดภัยไซเบอร์, ภัยคุกคามทางไซเบอร์
นักศึกษา ฐิติมา ภู่ห้อย
อาจารย์ที่ปรึกษาสารนิพนธ์ ดร.สุรชัย ทองแก้ว
อาจารย์ที่ปรึกษาสารนิพนธ์ร่วม ศาสตราจารย์.ดร.ประสงค์ ประณีตพลกรัง
หลักสูตร วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะ เทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
ปีการศึกษา 2564

บทคัดย่อ

การวิจัยนี้ มีวัตถุประสงค์เพื่อ 1) ศึกษาพฤติกรรมและความพร้อมของบุคลากรที่มีต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ 2) เพื่อวิเคราะห์และสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ และ 3) เพื่อพัฒนาแอปพลิเคชันสำหรับประเมินวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ โดยเป็นการวิจัยเชิงคุณภาพและการวิจัยเชิงปริมาณ การวิจัยเชิงคุณภาพนั้น ผู้วิจัยได้ศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง และสัมภาษณ์เชิงลึกผู้เชี่ยวชาญ จำนวน 15 คน และการสนทนากลุ่มกับผู้ปฏิบัติงานเกี่ยวข้องกับระบบเครือข่าย การวิจัยเชิงปริมาณ กลุ่มตัวอย่างที่ใช้ในการศึกษา คือ กลุ่มบุคลากรของสำนักการวางผังและพัฒนาเมือง กรุงเทพมหานคร ผลการวิจัยพบว่า การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์นั้นประกอบด้วย 3 องค์ประกอบหลักคือ ผู้บริหาร บุคลากรทุกระดับและระบบการจัดการด้านความมั่นคงปลอดภัยไซเบอร์ ด้วยการมีส่วนร่วมของบุคลากรที่สอดคล้องในแนวทางเดียวกันจึงจะเกิดการสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรที่ยั่งยืน และประเมินผลด้วยแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ของสำนักการวางผังและพัฒนาเมือง ทั้งนี้ เพื่อเป็นแนวทางในการสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรต่อไป

THEMATIC TITLE DEVELOPING A CYBERSECURITY CULTURE FRAMEWORK IN ORGANIZATIONS FOR CYBERSECURITY TRANSFORMATION
KEYWORDS Cybersecurity Culture, Cyber Threats
STUDENT THITIMA PHUHOY
ADVISOR DR.SURACHAI THONGKAEW
CO-ADVISOR PROFESSOR DR.PRASONG PRANEETPOLGRANG
LEVEL OF STUDY MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
FACULTY SCHOOL OF INFORMATION TECHNOLOGY, SRIPATUM UNIVERSITY
ACADEMIC YEAR 2021

ABSTRACT

The objectives of this research aimed to 1. Study the behavior and readiness of personnel towards cyber security 2. To analyze and create a cybersecurity culture within the organization for the transformation of cybersecurity and 3. To develop an application for assessing cybersecurity culture within the organization for the transformation of cybersecurity. This research use both a qualitative research and a quantitative research. For the qualitative research, the researcher studied related documents and related research. Including in-depth interviews with 15 experts and hold group conversations with network-related operators. For the quantitative research, the researcher works with the sample group of staffs of the City Planning and Urban Development Department, Bangkok. The results revealed that create a cybersecurity culture within the organization consists of 3 main components: directors, officers at all levels and Cyber Security Management Systems. With the participation of the people who are consistent in the same way, a sustainable organizational cybersecurity culture framework is created. Then evaluated with an application for assessing the organization's cybersecurity culture framework for the cybersecurity transformation of the City Planning and Urban Development Department. This can be a guideline for building a cybersecurity culture in the organization.

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้ประสบความสำเร็จลุล่วงได้ด้วยดี ด้วยความเมตตาจากท่าน ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง อาจารย์ที่ปรึกษาสารนิพนธ์ ที่ได้ให้ความกรุณาตั้งแต่ การสอนความรู้ด้านวิชาการ วิชาชีพ และวิชาชีวิต ท่านได้เน้นให้นักศึกษามีคุณธรรม จริยธรรม มีทัศนคติที่ดีต่อสังคม และการพัฒนาความสัมพันธ์ในรุ่น M.S.IT.26 ให้มีความผูกพันกันอย่างแน่นแฟ้น รวมทั้งท่านยังเป็นผู้สร้างแรงบันดาลใจและสร้างกำลังใจให้กับผู้วิจัยได้ทำตามที่ฝันและสามารถไปได้เกินกว่าที่ฝันไว้ อย่างไรก็ดี แม้ว่าการเรียนการวิจัยที่ค่อนข้างเข้มข้น แต่ท่านยังได้เมตตาให้เวลา ให้คำแนะนำอย่างจริงจังและต่อเนื่องจนการทำสารนิพนธ์ประสบความสำเร็จอย่างดียิ่ง ตลอดระยะเวลาในการทำสารนิพนธ์ฉบับนี้ ท่านได้ให้คำปรึกษา ข้อแนะนำ ให้แนวทางในการปรับปรุงแก้ไขงานวิจัย ส่งเสริมการนำเสนอผลงานในการประชุมวิชาการระดับชาติ ท่านสอนการวางแผนเตรียมการและซักซ้อม ทำให้นักศึกษามีความพร้อม มั่นใจ และมีกำลังใจมากขึ้นก่อนการขึ้นสอบหรือนำเสนองานวิจัย ผู้วิจัยรู้สึกซาบซึ้งและประทับใจเป็นอย่างมาก จึงขอกราบขอบพระคุณท่านอาจารย์เป็นอย่างสูงมา ณ โอกาสนี้

ขอขอบพระคุณ ดร.สุรชัย ทองแก้ว อาจารย์ที่ปรึกษาสารนิพนธ์ที่คอยให้คำปรึกษา ข้อแนะนำ และคอยชี้แนะข้อผิดพลาดเพื่อปรับปรุงแก้ไขให้สารนิพนธ์ฉบับนี้มีความสมบูรณ์มากยิ่งขึ้น

ขอขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.สุรศักดิ์ มังสิงห์ ที่ให้แนวคิดข้อแนะนำในขั้นตอนของการทำสารนิพนธ์ รวมไปถึงให้คำแนะนำในการนำเสนอผลงานเพื่อให้การนำเสนอผลงานออกมาตรงประเด็นและมีความชัดเจนน่าเชื่อถือมากขึ้น

ขอขอบพระคุณคณบดีและคณาจารย์หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศทุกท่าน ที่ได้ประสิทธิ์ประสาทความรู้อันเป็นสิ่งสำคัญและส่งผลให้ผู้วิจัยได้นำความรู้มาประยุกต์ใช้ในการจัดทำสารนิพนธ์นี้

ขอขอบคุณเพื่อน ๆ ในรุ่น M.S.IT.26 ที่รักทุกคนที่คอยสนับสนุน ห่วงใย และให้กำลังใจช่วยเหลือกันอย่างดีเสมอมา

ขอขอบพระคุณครอบครัวและนางสาวโกเมน เตียงเกตุ ที่เป็นกำลังใจสำคัญและให้การสนับสนุนในด้านการเงินตลอดการศึกษา รวมทั้งขอขอบคุณหน่วยงานที่สนับสนุนทุนการศึกษา สำหรับข้อบกพร่องต่าง ๆ ที่อาจจะเกิดขึ้นนั้น ผู้วิจัยยินดีที่จะรับฟังคำแนะนำจากทุกท่าน และเคารพในทุกความเห็น ขอน้อมรับทุกข้อแนะนำเพื่อนำไปปรับปรุงตนเองและงานวิจัยในโอกาสต่อไป

ฐิติมา ภู่ห้อย

สิงหาคม 2565

สารบัญ

สารบัญ (ต่อ)

บทที่ **หน้า**

สารบัญ(ต่อ)

บทที่ **หน้า**

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญภาพ

ภาพประกอบที่ **หน้า**

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.2562 กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน รวมทั้งกำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล จึงจำเป็นต้องกำหนดให้มีธรรมาภิบาลข้อมูลภาครัฐเพื่อเป็นหลักการและแนวทางในการดำเนินการให้เป็นไปตามพระราชบัญญัติดังกล่าว อันจะนำไปสู่การพัฒนาระบบข้อมูลที่สำคัญของภาครัฐเพื่อประโยชน์ในการกำหนดหลักเกณฑ์และวิธีการเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลของหน่วยงานของรัฐอย่างเป็นระบบ ตลอดจนการพัฒนาศูนย์กลางข้อมูลเปิดภาครัฐ เพื่อให้ประชาชนสามารถเข้าถึงและใช้ประโยชน์ได้อย่างมีประสิทธิภาพ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 มาตรา 5 และมาตรา 9 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553 กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษรตลอดจนเพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ ของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

สำนักการวางผังและพัฒนาเมือง กรุงเทพมหานคร จึงได้นำเอาเทคโนโลยีสารสนเทศเข้ามาสนับสนุนเพื่อเพิ่มประสิทธิภาพในการดำเนินงานตามภารกิจหลักในการวางผังและจัดทำผังเมืองกรุงเทพมหานคร วางแผนพัฒนาพื้นที่ จัดทำมาตรการทางผังเมือง ดำเนินการอนุรักษ์และปรับปรุงฟื้นฟูเมือง รวมทั้งศึกษารวบรวมข้อมูล และจัดทำข้อมูลสารสนเทศเพื่อการบริหารจัดการเมืองเพื่อบริการประชาชน หน่วยงานภาครัฐ และหน่วยงานเอกชน เพื่อให้ได้บริการสารสนเทศที่ทันสมัย สะดวก รวดเร็ว

โดยสำนักงานภูมิสารสนเทศ สำนักการวางผังและพัฒนาเมือง กรุงเทพมหานคร ได้มีการจัดวางระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินภารกิจภายในองค์กร ในการบริการประชาชน หน่วยงานภาครัฐ และหน่วยงานเอกชน และเพื่อใช้เป็นศูนย์กลางในการเชื่อมโยงระบบสารสนเทศของกรุงเทพมหานคร และหน่วยงานภายในกรุงเทพมหานคร ได้แก่ ระบบสารสนเทศเพื่อการจัดการ (Management Information Systems: MIS) ระบบหนังสือเวียนกรุงเทพมหานคร ระบบภูมิสารสนเทศบนระบบเครือข่าย และรองรับระบบต่าง ๆ ที่จะเกิดขึ้นในอนาคต จากการให้บริการระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานนี้ ทำให้บุคลากรในหน่วยงานสามารถเข้าถึงระบบเครือข่ายได้ทั้งจากเครื่องคอมพิวเตอร์ โทรศัพท์ส่วนตัว สมาร์ตทีวี และอุปกรณ์อื่น ๆ ได้อย่างสะดวกและรวดเร็วมากขึ้น ข้อดีคือทำให้สามารถทำงาน สืบค้นข้อมูล ติดต่อสื่อสาร และให้บริการประชาชนได้สะดวก รวดเร็ว แต่ก็ทำให้เกิดความเสี่ยงต่อการนำไปใช้ในทางที่ผิดกฎหมาย ทั้งที่ตั้งใจหรือไม่ตั้งใจ และมีความเสี่ยง ที่จะเกิดภัยคุกคามจากผู้ไม่ประสงค์ดีในการก่ออาชญากรรมและแสวงผลประโยชน์ในรูปแบบต่าง ๆ จะเป็นเหยื่อจากภัยคุกคามจากอินเทอร์เน็ตหรือที่เรียกว่าภัยคุกคามทางไซเบอร์ได้ตลอดเวลาเช่นกัน

ผู้วิจัยจึงมีความสนใจในการศึกษาแนวทางที่จะเป็นการป้องกันและลดผลกระทบต่อความเสียหายอันเกิดจากภัยคุกคามทางไซเบอร์จากช่องทางต่าง ๆ รวมทั้งความเสียหายอันเกิดจากการทำงานผิดปกติของฮาร์ดแวร์ ซอฟต์แวร์ แฟ้มข้อมูลที่สำคัญ และเพื่อให้ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานใช้งานได้อย่างต่อเนื่อง สามารถป้องกันปัญหาการถูกโจมตีระบบเครือข่ายคอมพิวเตอร์และไม่ให้มีการใช้งานอินเทอร์เน็ตในทางที่ผิด หน่วยงานจึงจำเป็นที่จะต้องให้บุคลากรมีความรู้ ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ ซึ่งวิธีการหนึ่งที่จะทำให้บุคลากรมีความตระหนักถึงภัยคุกคามทางไซเบอร์นั้นคือการสร้างความเข้าใจอย่างถ่องแท้ให้กับบุคลากรทุกคนในเรื่องภัยคุกคามทางไซเบอร์ ทั้งนี้ เพื่อลดความเสี่ยงและภัยคุกคามทางไซเบอร์ด้วยการสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ให้เกิดขึ้นในองค์กร

1.2 คำถามการวิจัย

1.2.1 ความพร้อมของบุคลากรในองค์กรที่มีต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นอย่างไร

1.2.2 วัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ มีลักษณะอย่างไร

1.3 วัตถุประสงค์ของการวิจัย

1.3.1 เพื่อศึกษาพฤติกรรมและความพร้อมของบุคลากรที่มีต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

1.3.2 เพื่อวิเคราะห์และสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

1.3.3 เพื่อพัฒนาแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

1.4 สมมติฐานการวิจัย

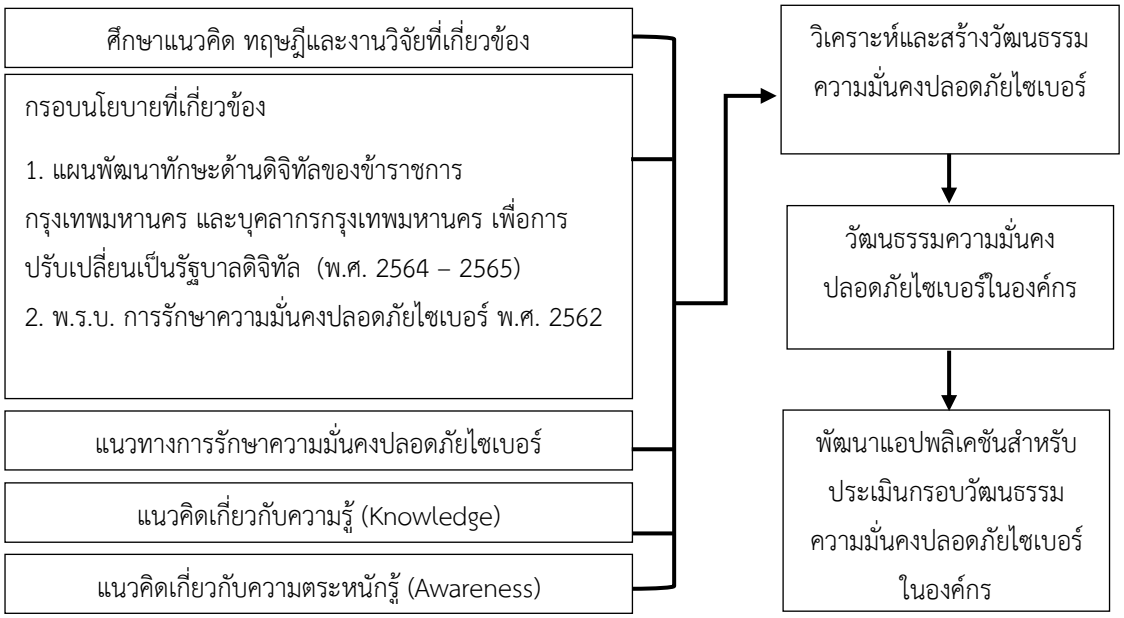
1.4.1 ความพร้อมของบุคลากรในองค์กรที่มีต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ มีค่าอยู่ในระดับมาก

1.4.2 กรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ มีความเหมาะสมอยู่ในระดับมาก

1.4.3 กรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ มีการยอมรับอยู่ในระดับมาก

1.5 กรอบแนวคิดในการวิจัย

จากการศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้อง จึงเสนอกรอบแนวคิดในการวิจัย ดังภาพประกอบที่ 1.1



ภาพประกอบที่ 1.1 กรอบแนวคิดในการวิจัย

1.6 ขอบเขตของการวิจัย

งานวิจัยเรื่อง “การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์” มีขอบเขตเนื้อหาในการวิจัยดังนี้

1.6.1 ขอบเขตด้านเวลา : ระยะเวลาในการทำวิจัยจากการศึกษา วิเคราะห์ ออกแบบและสรุปแนวทางในการกำหนดนโยบาย ใช้เวลา 1 ปีการศึกษา ตั้งแต่เดือนพฤศจิกายน พ.ศ.2564 ถึงเดือนตุลาคม พ.ศ. 2565

1.6.2 ขอบเขตด้านสถานที่/ประชากร : บุคลากรในสังกัดสำนักการวางผังและพัฒนาเมือง กรุงเทพมหานคร

1.6.3 ขอบเขตด้านเนื้อหาของการทำงานวิจัย ได้แก่ เอกสาร ระเบียบ คำสั่ง นโยบาย และแนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

1.7 ประโยชน์ที่ได้รับ

1.7.1 ทำให้ทราบถึง แนวทาง กระบวนการ และมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

1.7.2 ทำให้ทราบถึงความพร้อมของบุคลากรในการรับมือต่อภัยคุกคามทางไซเบอร์

1.7.3 ได้แอปพลิเคชันสำหรับประเมินวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร

1.8 นิยามศัพท์

1.8.1 วัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ หมายถึง คุณลักษณะ ทัศนคติ ของบุคลากรและองค์กร เพื่อสนับสนุน เสริมสร้าง รวมทั้งทำให้เกิดความยั่งยืนด้านความมั่นคงปลอดภัยไซเบอร์

1.8.2 การเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Transformation) หมายถึง กระบวนการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ เป็นการเปลี่ยนทัศนคติและสร้างวัฒนธรรมทางความมั่นคงปลอดภัยไซเบอร์ที่หยั่งรากลึกในระดับบุคคลและองค์กรให้เกิดภูมิคุ้มกัน และมีจริยธรรมทางความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้เพื่อสร้างความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ อีกทั้งยังทำให้บุคคลและองค์กรมีขีดความสามารถด้านไซเบอร์ ในอันที่จะป้องกัน ต่อต้าน ตรวจจับ และตอบสนองต่อการบุกรุก การจารกรรม หรือการหลอกลวง ที่จะทำให้เกิดความเสียหายได้

1.8.3 ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) หมายถึง ภาวะพ้นจากภัยคุกคามที่มีต่อเครือข่ายระบบคอมพิวเตอร์ โปรแกรม และข้อมูล เพื่อรักษาไว้ซึ่งลักษณะสำคัญ 3 ประการ คือ ความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน ภาวะดังกล่าวจะเกิดขึ้นได้ ต้องอาศัยบุคลากร

กระบวนการทำงาน และเครื่องมือที่เหมาะสม (ราชบัณฑิตสาขาคอมพิวเตอร์และเทคโนโลยีสารสนเทศ, 2558)

1.8.4 ไซเบอร์ (Cyber) หมายถึง คำที่ใช้เติมหน้าคำอื่นเพื่อแสดงความเกี่ยวข้องกับเครือข่ายคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือ อินเทอร์เน็ต หรือความเป็นจริงเสมือน (Virtual Reality) เช่น ไซเบอร์สเปซ (Cyberspace) หมายถึง สภาพแวดล้อมสมมติในเครือข่ายอินเทอร์เน็ต (ราชบัณฑิตสาขาคอมพิวเตอร์และเทคโนโลยีสารสนเทศ, 2559)

1.9 สรุป

ในบทที่ 1 นี้การเริ่มต้นการทำวิจัย โดยเป็นการนำแสนอของความเป็นมาและความสำคัญของปัญหา คำถามการวิจัย วัตถุประสงค์ของการวิจัย สมมติฐานการวิจัย กรอบแนวคิดในการวิจัย ขอบเขตของการวิจัย ประโยชน์ที่ได้รับ และนิยามศัพท์ เพื่อเป็นแนวทางการในดำเนินการวิจัยต่อไป

บทที่ 2

แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

การวิจัย เรื่อง “การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์” นี้ ผู้วิจัยได้ศึกษาแนวคิด ทฤษฎี เอกสารทางวิชาการ แผนพัฒนาของกรุงเทพมหานคร และศึกษาเอกสารงานวิจัยที่เกี่ยวข้องเพื่อเป็นแนวทางในการวิจัย มุ่งวิเคราะห์ความรู้ ความเข้าใจของบุคลากรในหน่วยงานในการใช้ระบบเครือข่ายและมีพฤติกรรมเสี่ยงต่อภัยคุกคามไซเบอร์ เพื่อกำหนดแนวทางในการสร้างวัฒนธรรมความมั่งคงปลอดภัยไซเบอร์ในองค์กรต่อไป ดังนี้

2.1 แผนพัฒนาทักษะด้านดิจิทัลของข้าราชการกรุงเทพมหานครและบุคลากรกรุงเทพมหานคร เพื่อการปรับเปลี่ยนเป็นรัฐบาลดิจิทัล ระยะเริ่มแรก (Early) (พ.ศ. 2564 – 2565)

2.2 พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2.3 มาตรฐานสากลที่เกี่ยวข้อง

2.4 แนวคิดเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

2.5 แนวคิดเกี่ยวกับการคุกคามทางไซเบอร์ (Cyber Threat)

2.6 แนวคิดด้านวัฒนธรรม

2.7 แนวคิดเกี่ยวกับวัฒนธรรมองค์กร (Organizational Culture)

2.8 แนวคิดเกี่ยวกับความรู้ (Knowledge) ด้านความมั่นคงปลอดภัยไซเบอร์

2.9 แนวคิดเกี่ยวกับความตระหนักรู้ (Awareness)

2.10 งานวิจัยที่เกี่ยวข้อง

2.11 สรุป

2.1 แผนพัฒนาทักษะด้านดิจิทัลของข้าราชการกรุงเทพมหานครและบุคลากรกรุงเทพมหานคร เพื่อการปรับเปลี่ยนเป็นรัฐบาลดิจิทัล ระยะเริ่มแรก (Early) (พ.ศ.2564– 2565)

ด้วยสถาบันพัฒนาข้าราชการกรุงเทพมหานครได้จัดทำแผนพัฒนาทักษาด้านดิจิทัลของข้าราชการกรุงเทพมหานครและบุคลากรกรุงเทพมหานคร เพื่อการปรับเปลี่ยนเป็นรัฐบาลดิจิทัล ระยะเริ่มแรก (Early) โดยจัดทำคู่มือการพัฒนาให้หน่วยงานในสังกัดกรุงเทพมหานครนำไปใช้เป็น

แนวทางในการพัฒนาบุคลากรของหน่วยงาน เพื่อสร้างความพร้อมในการเป็นรัฐบาลดิจิทัลของกรุงเทพมหานครต่อไป

1. กำหนดแนวทางการพัฒนาที่ครอบคลุมทุกกลุ่มภารกิจ แบ่งเป็น 4 ด้าน ดังนี้

1.1 พัฒนาทักษะดิจิทัลด้านการบริหารและการอำนวยการ สำหรับกลุ่มภารกิจผู้บริหารระดับสูง (Executive) และผู้อำนวยการ (Management)

เป้าประสงค์ นักบริหารของกรุงเทพมหานครได้รับการพัฒนาทักษะการนำองค์กรสู่การเป็นรัฐบาลดิจิทัล

1.2 พัฒนาทักษะดิจิทัลด้านงานนโยบาย การจัดการข้อมูลสารสนเทศและการพัฒนาองค์กร สำหรับกลุ่มภารกิจผู้ทำงานด้านนโยบายและวิชาการ (Academic) และผู้ปฏิบัติงานอื่น (Others)

เป้าประสงค์ ทรัพยากรบุคคลของกรุงเทพมหานครมีความรู้และทักษะในการใช้เทคโนโลยีดิจิทัลที่ทันสมัย สามารถวิเคราะห์ใช้ข้อมูลสารสนเทศเพื่อปฏิบัติงานได้

1.3 พัฒนาทักษะดิจิทัลด้านการให้บริการ สำหรับกลุ่มภารกิจผู้ทำงานด้านบริการ (Service)

เป้าประสงค์ ทรัพยากรบุคคลของกรุงเทพมหานครมีความรู้ด้านให้บริการดิจิทัลภาครัฐ ที่พร้อมพัฒนาไปสู่การให้บริการที่ทันสมัย

1.4 พัฒนาทักษะดิจิทัลเพื่อการพัฒนาโครงสร้างพื้นฐานและงานด้านเทคโนโลยีดิจิทัลสำหรับกลุ่มภารกิจผู้ปฏิบัติงานเฉพาะด้านเทคโนโลยี (Technologist)

เป้าประสงค์ ผู้ปฏิบัติงานด้านเทคโนโลยีดิจิทัลของกรุงเทพมหานคร ได้รับการพัฒนาความรู้และทักษะการจัดการเทคโนโลยี เพื่อการประยุกต์ใช้ภายในองค์กร และการจัดบริการของกรุงเทพมหานคร พร้อมปรับเปลี่ยนเป็นรัฐบาลดิจิทัล

2. การจำแนกกลุ่มข้าราชการกรุงเทพมหานครและบุคลากรกรุงเทพมหานคร แบ่งเป็น 6 กลุ่มภารกิจ

2.1 กลุ่มภารกิจผู้บริหารระดับสูง (Executive)

2.2 กลุ่มภารกิจผู้อำนวยการ (Management)

2.3 กลุ่มภารกิจผู้ทำงานด้านนโยบายและวิชาการ (Academic)

2.4 กลุ่มภารกิจผู้ปฏิบัติงานอื่น (Others)

2.5 กลุ่มภารกิจผู้ทำงานด้านบริการ (Service)

2.6 กลุ่มภารกิจผู้ปฏิบัติงานเฉพาะด้านเทคโนโลยี (Technologist)

3. กำหนดหลักสูตรการพัฒนาความสามารถด้านดิจิทัล เป็น 4 หมวด ดังนี้

หมวดที่ 1 รู้เท่าทันและใช้เทคโนโลยีเป็น (Digital Literacy : DLit)

หมวดที่ 2 เข้าใจนโยบาย กฎหมายและมาตรฐาน (Digital Governance, Standard and Compliance : DG)

หมวดที่ 3 ใช้ดิจิทัลเพื่อการประยุกต์และพัฒนา (Digital Technology & Digital Process and Service Design : DT & DS)

หมวดที่ 4 ใช้ดิจิทัลเพื่อการวางแผนบริหารจัดการ และนำองค์กร (Strategic and Project Management & Digital Leadership : SPM & DL)

หมวดที่ 5 ใช้ดิจิทัลเพื่อขับเคลื่อนการเปลี่ยนแปลงและสร้างสรรค์ (Digital Transformation : DTr)

จากการตรวจสอบโครงสร้างหน่วยงาน บุคลากรในหน่วยงาน ประกอบไปด้วยทุกกลุ่มภารกิจ ที่ต้องมีการพัฒนาทักษะด้านดิจิทัลในการใช้งานดิจิทัลเพื่อความมั่นคงปลอดภัย ตั้งแต่การกำหนดนโยบายการใช้ดิจิทัลได้ถูกต้องตามกฎหมาย การใช้อินเตอร์เน็ตอย่างปลอดภัย การป้องกันภัยคุกคาม การจัดการภัยคุกคามด้านความมั่นคงปลอดภัย การปฏิบัติตามหลักการเพื่อรักษาความปลอดภัย

2.2 พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลบังคับใช้แล้ว ตั้งแต่วันที่ 28 พฤษภาคม 2562 เป็นกลไกการเฝ้าระวัง ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มีการประสานความร่วมมือระหว่างผู้เกี่ยวข้องพัฒนาความรู้ความสามารถของบุคลากรและผู้เชี่ยวชาญ รวมถึงการให้ความรู้และความตระหนักถึงภัยไซเบอร์ เช่น ไวรัส มัลแวร์ อาชญากรทางคอมพิวเตอร์ที่อาจเกิดกับระบบโครงสร้างพื้นฐานทางสารสนเทศสำคัญและส่งผลเสียหายในระดับประเทศ Critical Infrastructures (CI)

หน่วยงาน หรือองค์กร หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงาน หรือองค์กรที่เป็นโครงสร้างพื้นฐานสำคัญของประเทศมีธุรกรรมทางอิเล็กทรอนิกส์ที่ส่งผลสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณชน ได้แก่ กลุ่มความมั่นคงของรัฐ กลุ่มบริการภาครัฐที่สำคัญ กลุ่มการเงินการ-ธนาคาร กลุ่มเทคโนโลยีสารสนเทศ กลุ่มพลังงาน กลุ่มสาธารณูปโภค และกลุ่มสาธารณสุข Critical Information Infrastructure (CII)

ระบบสารสนเทศของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศที่ใช้ในการดำเนินงานและให้บริการ หากระบบถูกรบกวนจะทำให้ไม่สามารถดำเนินงานหรือให้บริการได้

ส่วนประกอบของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

หมวด 1 จัดตั้งคณะกรรมการ

- คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.)

- คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ (กกช.)
- คณะกรรมการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (กสส.)

หมวด 2 จัดตั้งสำนักงาน

จัดตั้งสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและคณะกรรมการกำกับดูแลสำนักงาน

หมวด 3 กำหนดแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์

- กำหนดกรอบนโยบายและแผน
- แนวทางการบริหารจัดการ
- กำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศและแนวทางการประสานงาน
- แนวทางการรับมือภัยคุกคามทางไซเบอร์

หมวด 4 กำหนดบทลงโทษ

- บทกำหนดโทษเจ้าหน้าที่และพนักงานสอบสวน
- บทกำหนดโทษหน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ
- บทกำหนดโทษผู้กระทำความผิด ฝ่าฝืน ขัดขวางและไม่ปฏิบัติตามคำสั่งคณะกรรมการ

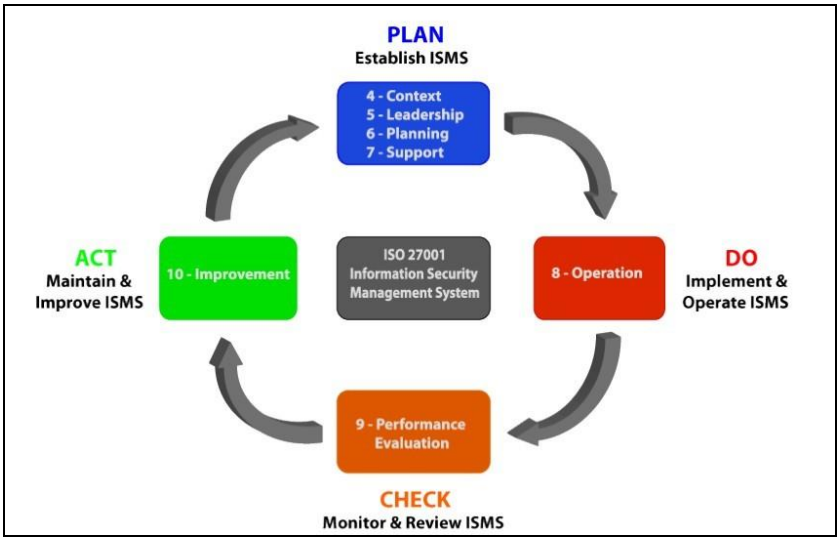
2.3 มาตรฐานสากลที่เกี่ยวข้อง

1. ระบบมาตรฐานด้านความปลอดภัยสารสนเทศ ISO 27001 หรือ ISO/IEC 27001:2013 (Information Security Management System: ISMS) เป็น มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งใช้หลักการพื้นฐานของความมั่นคงปลอดภัยสารสนเทศ (Information Security) ที่มีองค์ประกอบ 3 ส่วน ได้แก่ C (Confidentiality), I (Integrity), A (Availability)

มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานสากลของค่าย ISO (The International Organization for Standardization) และ IEC (The International Electrotechnical Commission) โดยมีวิวัฒนาการมาจากมาตรฐาน BS 7799, ISO/IEC 17799 : 2000, ISO/IEC 17799:2005, ISO/IEC 27001:2005, ISO/IEC 27001:2013 ตามลำดับ ซึ่งเป็นมาตรฐานการจัดการข้อมูลที่สำคัญ เพื่อธุรกิจดำเนินไปอย่างต่อเนื่อง มาตรฐานเหล่านี้เป็นมาตรฐานสากล ที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัย ให้กับระบบสารสนเทศขององค์กร

ระบบ ISMS มีการประยุกต์ใช้หลักการ PDCA (Plan- Do -Check- Action) ซึ่งเป็นหลักการบริหารจัดการที่ใช้กันแพร่หลาย และทั้งนี้ EGA เล็งเห็นถึงความสำคัญของการรักษาความมั่นคงปลอดภัย สารสนเทศที่ใช้หลักการ PDCA จึงกำหนดมาตรฐานการดำเนินการให้สอดคล้องตามมาตรฐานสากล ISO/IEC 27001:2013 อาทิเช่น การจัดทำนโยบาย กระบวนการ การกำหนด

หน้าที่ ความรับผิดชอบ การควบคุม การตรวจสอบ การประเมินความเสี่ยง การวางแผนความต่อเนื่องทางธุรกิจ การจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยและสิ่งบกพร่อง เป็นต้น และเมื่อเดือนมิถุนายน 2560 ที่ผ่านมา EGA ได้ผ่านการรับรองตามมาตรฐานสากล ISO/IEC 27001:2013 สำหรับบริการ G-Cloud ในขอบเขตการขอรับรอง : การบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศสำหรับบริการ G-Cloud ในระดับ Infrastructure as a service ดังภาพประกอบที่ 2.1



ภาพประกอบที่ 2.1 โครงสร้างหลักการ PDCA (Plan- Do -Check- Action)

ในการบริหารจัดการให้องค์กรทำมาตรฐาน ISO/IEC 27001 ในหลัก PDCA (Plan - Do - Check - Action) ต้องมีความเข้าใจใน 2 เรื่องใหญ่ ๆ คือ

- เข้าใจองค์กรตนเอง : ต้องสำรวจข้อมูล ซอฟต์แวร์ ฮาร์ดแวร์ บุคลากร ในขอบเขตที่จัดทำระบบ ข้อมูลยิ่งมีรายละเอียดมากยิ่งเป็นสิ่งที่ดี ทะเบียนทรัพย์สินเป็นจุดเริ่มต้นที่ดีในการรวบรวมข้อมูลเข้าใจภารกิจขององค์กร รู้ว่าระบบงานใดสำคัญที่สุดและระบบงานต่าง ๆ มีข้อจำกัดและจุดอ่อนอะไร เพื่อที่จะหามาตรการมาจัดการกำจัดจุดอ่อน เช่น ระบบฐานข้อมูลทำงานอยู่บน Server ที่เก่า ใช้มานาน (ไม่มีค่าเสื่อมของครุภัณฑ์) มีการจัดเก็บข้อมูลจนเกือบไม่มีพื้นที่ว่าง และหากชำรุดก็ไม่สามารถดำเนินการซ่อมแซมได้ ในกรณีนี้จุดอ่อน คือ Server มีความเสี่ยงที่จะชำรุดหรือหยุดการทำงานได้ทุกเมื่อ ดังนั้น องค์กรต้องหามาตรการในการจัดการความเสี่ยง โดยการเสนอของบประมาณในการจัดหาอุปกรณ์ทดแทน หรือ ระบบคลาวด์ เพื่อย้ายข้อมูลไปจัดเก็บที่อุปกรณ์ใหม่ก่อนที่จะไม่สามารถเปิด Server นั้นขึ้นมาใช้งานข้อมูลได้

- เข้าใจมาตรฐาน : การจะนำมามาตรฐานมาใช้งาน ย่อมจะต้องทำความเข้าใจในมาตรฐานนั้นก่อน เข้าใจว่าต้องทำอะไร ต้องเตรียมการอย่างไร จัดทำเอกสาร (Documents) อะไร และการนำไปใช้งานจริง (Implementation) การทำระบบให้มีประสิทธิภาพ ต้องทำตาม

หัวใจหลักของกระบวนการระบบบริหารจัดการด้านความมั่นคงปลอดภัย มาตรฐาน ISO/IEC27001 ซึ่งประกอบด้วย 4 ขั้นตอนหลัก PDCA (Plan - Do - Check - Action) กล่าวคือ

1. การวางแผน (Plan) คือ การวางแผนดำเนินการตามกระบวนการ ขั้นตอนแรกองค์กรต้องระบุขอบเขตและนโยบายการสร้างความมั่นคงปลอดภัยขององค์กร และทำการประเมินความเสี่ยงตามขอบเขตและนโยบายที่ได้ระบุไว้ เพื่อให้สามารถระบุความเสี่ยงที่มีอยู่ และพิจารณาแนวทางในการจัดการความเสี่ยงนั้น รวมทั้งระบุความเสี่ยงที่หลงเหลือให้อยู่ในระดับที่องค์กรยอมรับได้

2. การปฏิบัติตาม (Do) คือ การวางแผนดำเนินการจัดความเสี่ยงตามแนวทางจัดการความเสี่ยงที่ได้จากขั้นตอนแรก ระบุวิธีพิจารณาประสิทธิภาพของแนวทางจัดการความเสี่ยง และสร้างความตระหนักในการปฏิบัติตามแนวทางจัดการความเสี่ยง เพื่อให้แนวทางจัดการความเสี่ยงไปอย่างมีประสิทธิภาพ

3. การตรวจสอบ (Check) คือ การเฝ้าระวังแนวทางจัดการความเสี่ยงที่ได้ดำเนินการไปและทบทวนประสิทธิภาพของแนวทางจัดการความเสี่ยงตามแนวทางที่ได้ระบุไว้ รวมถึงดำเนินการประเมินความเสี่ยงและตรวจสอบกระบวนการตามระยะเวลาที่เหมาะสม โดยให้สอดคล้องกับการเปลี่ยนแปลงที่สำคัญของสารสนเทศหรือการเปลี่ยนแปลงขององค์กร ขั้นตอนในการติดตามการดำเนินการตามแผน คือ การติดตามเพื่อดูว่าการพัฒนาระบบงานว่าเป็นไปตามที่ได้วางแผนหรือไม่ เช่น ระบบงานต้องทำงานได้ครบถ้วนตามข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดไว้

4. ปรับปรุงแก้ไข (Act) คือ การที่เมื่อตรวจสอบ (Check) ในทุกรายการแล้วและพบปัญหาที่ต้องทำการแก้ไข ให้ดำเนินการเพิ่มเติมตามที่เห็นสมควร (Act) เช่น กรณีตรวจสอบพบว่า ระบบงานไม่มีการดำเนินการสำรองข้อมูล ให้ดำเนินการแก้ไข (Take action) เพื่อให้ระบบสามารถจัดการดำเนินการตามแผนและดำเนินการเพิ่มเติมตามที่เห็นสมควร ถ้ายังมีความเสี่ยงใหม่หรือเพิ่มเติมอยู่ต้องวางแผนลดความเสี่ยงนั้น (Take Action)

โดยสรุปวงจร PDCA (Plan- Do -Check- Action) จึงเริ่มต้นตั้งแต่เริ่มมีทรัพย์สินสารสนเทศถูกนำมาใช้งานในองค์กร ต้อง Check และ Action อย่างต่อเนื่อง ตั้งแต่มีการติดตั้งจนกระทั่งทรัพย์สินนั้นจะหมดอายุการใช้งาน จึงยุติการประเมินความเสี่ยงสำหรับทรัพย์สินเหล่านั้น

2. NIST Cybersecurity Framework เป็นหนึ่งในกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ซึ่งเป็นที่นิยมใช้อย่างมากในปัจจุบัน ไม่เพียงแค่องค์กรในสหรัฐฯ เท่านั้น Framework ดังกล่าว ยังเป็นที่แพร่หลายไปยังทุกภูมิภาคทั่วโลก รวมไปถึงประเทศไทย หลายองค์กรเริ่มนำ Framework นี้ประยุกต์ใช้เพื่อรับมือกับภัยคุกคามไซเบอร์

Framework นี้นำเสนอหลักการและแนวทางปฏิบัติที่ดีที่สุดของการบริหารจัดการความเสี่ยง เพื่อยกระดับความมั่นคงปลอดภัยขององค์กรทุกระดับ รวมไปถึงช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ โดยหัวใจสำคัญของ Framework แบ่งออกเป็น 5 ฟังก์ชันหลัก ดังภาพประกอบที่ 2.2

ภาพประกอบที่ 2.2 กรอบการรักษาความมั่นคงปลอดภัย (NIST Cybersecurity Framework)

1. การระบุ – Identify เข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยง เป็นขั้นตอนแรกในการศึกษาทำความเข้าใจบริบท ทรัพยากร และกิจกรรมงานสำคัญ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูลและขีดความสามารถในการจัดการ

2. การป้องกัน – Protect การวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร เป็นการจัดทำและดำเนินตามมาตรการป้องกันที่เหมาะสมสำหรับการให้บริการโครงสร้างพื้นฐาน โดยมีวัตถุสำคัญเพื่อจำกัดผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุมการฝึกอบรมและการสร้างความตระหนัก มาตรการควบคุมการเข้าถึง และมาตรการด้านความปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนการควบคุมด้านเทคโนโลยี

3. การตรวจจับ – Detect การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ ตรวจหาเหตุการณ์ด้านความมั่งคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวังหรือตรวจติดตามต่อเนื่อง

4. การตอบสนอง – Respond การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น เป็นการจัดทำเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุง

5. การคืนสภาพ – Recovery การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม

2.4 แนวคิดเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแหงชาติ (สวทช. หรือ NSTDA) ให้ความหมายของไซเบอร์ (Cyber) ว่าเป็นคำที่กร่อนมาจากคำว่า ไซเบอร์เนติกส์ (Cybernetics) และมีความหมายที่เกี่ยวกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต (Internet) และยังมีการให้ความหมายว่าคือ “สารสนเทศ (Virtual) เสมือนจริงที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง”

โดยรวมแล้วไซเบอร์จึงเป็นความหมายในเชิงนามธรรม หมายถึง ขอบเขตที่เกี่ยวข้องกับการใช้งานของระบบเครือข่ายคอมพิวเตอร์ หรือระบบอิเล็กทรอนิกส์ ซึ่งจะครอบคลุมมากกว่าคอมพิวเตอร์ซึ่งมีความหมายในเชิงรูปธรรมของอุปกรณ์ระบบคอมพิวเตอร์ทั่วไป

การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ตามพจนานุกรม Cyberspace Operations Lexicon ของ กระทรวงกลาโหมสหรัฐฯ คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ (ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ), ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล และกระจายข้อมูล ทั้งนี้ ยังรวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม อุบัติเหตุ และความผิดพลาดต่างๆ ความเสี่ยงของการรักษาความปลอดภัยของไซเบอร์อาจรวมถึงสิ่งต่าง ๆ ที่ทำลายความเชื่อมั่นและความไว้วางใจของผู้ถือผลประโยชน์ร่วม (Stakeholder), ผลกระทบที่มีต่อการเก็บรักษาและการเติบโตของกลุ่มลูกค้า, การละเมิดการป้องกันข้อมูลส่วนตัวของกลุ่มลูกค้าและผู้ถือหุ้น, การรบกวนการทำงานหรือการดำเนินธุรกรรม, ผลกระทบที่เป็นปฏิปักษ์ต่อชีวิตและสุขภาพของผู้ปฏิบัติงาน และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ

ความเสี่ยงของความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) อาจรวมถึงสิ่งต่าง ๆ ที่ทำลายความเชื่อมั่นและความไว้ใจของผู้มีสวนได้เสีย (Stakeholder) ผลกระทบที่มีต่อการเก็บรักษาและการเติบโตของกลุ่มลูกค้า การละเมิดการป้องกันข้อมูลสวนตัวของกลุ่มลูกค้าและผู้ถือหุ้น การรบกวนการทำงานหรือการดำเนินธุรกรรม ผลกระทบที่เป็นปฏิปักษ์ต่อชีวิตและสุขภาพของผู้ปฏิบัติงาน และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ

2.5 แนวคิดเกี่ยวกับการคุกคามทางไซเบอร์ (Cyber Threat)

การคุกคามทางไซเบอร์สามารถเกิดขึ้นได้หลายรูปแบบแต่ละรูปแบบสามารถสร้างความเสียหายให้แก่บุคคล เศรษฐกิจ ไปจนถึงโครงสร้างพื้นฐานของประเทศต่าง ๆ ภัยคุกคามอาจเป็นการก่อวินาศกรรม การจารกรรมข้อมูลหรือรหัสสำคัญ การปล่อยข้อมูลลวง การทำลายชื่อเสียงของประเทศ องค์กร หรือบุคคล การเผยแพร่ข่าวสารอันเป็นเท็จ รวมถึงการทำลายระบบปฏิบัติการของเซิร์ฟเวอร์คอมพิวเตอร์ส่วนบุคคล และอุปกรณ์เคลื่อนที่ เช่น แท็บเล็ต หรือโทรศัพท์แบบสมาร์ตโฟน

2.5.1 ประเภทของการเกิดภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์สามารถแบ่งออกได้ ดังนี้

1. ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์

โปรแกรมประยุกต์ (Application-Based Threats) ที่ถูกดาวน์โหลดมาเพื่อติดตั้งบนคอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ อาจจะถูกแอบแฝงมาด้วยโปรแกรมที่เป็นภัยคุกคาม ภัยคุกคามประเภทนี้เรียกว่า มัลแวร์ (Malware) : ซึ่งเป็นโปรแกรมที่ถูกออกแบบมาเพื่อทำอันตรายต่อข้อมูลในคอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ ทำให้เกิดความขัดข้องหรือเสียหายกับระบบปฏิบัติการ นอกจากนี้โปรแกรมที่ติดมัลแวร์ยังส่งข้อความที่ไม่พึงประสงค์ออกไปยังผู้อื่น หรือขโมยข้อมูลสำคัญออกไปตัวอย่างโปรแกรมในกลุ่มนี้ ได้แก่ Virus, Worm, Trojan, Botnet หรือ Spyware เป็นต้น

2. ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์

ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ (Web-Based Threats) เป็นภัยคุกคามที่เกิดจากการที่ผู้ใช้คอมพิวเตอร์หรืออุปกรณ์พกพา เปิดเว็บไซต์ขึ้นมาใช้งาน ซึ่งเว็บไซต์ที่เรียกมาใช้อาจเป็นเว็บไซต์ฟิชชิ่ง (Phishing) ซึ่งถูกออกแบบให้มีลักษณะคล้ายคลึงกับเว็บไซต์จริงเพื่อหลอกให้ผู้ใช้กรอกข้อมูลเข้าสู่ระบบของผู้ไม่หวังดีเช่น หลอกให้ผู้ใช้งานล็อกอินเข้าอีเมล เฟซบุ๊ก หรือเว็บไซต์ที่เกี่ยวของกับธุรกรรมทางการเงิน ซึ่งจะคอยดักจับรหัสล็อกอินของผู้ใช้งานนั้น ๆ ทำให้ข้อมูลหรือบัญชีการใช้งานนั้น ๆ มีความเสี่ยงที่จะโดนขโมยข้อมูลออก

3. ภัยคุกคามจากการใช้งานเครือข่ายไร้สาย

ปัจจุบันมีผู้ให้บริการเครือข่ายไร้สายเป็นจำนวนมาก มีทั้งที่น่าเชื่อถือและที่ไม่น่าเชื่อถือรวมถึงผู้ที่แอบแฝงเพื่อวัตถุประสงค์อื่น ดังนั้นผู้ใช้คอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่เชื่อมต่อระบบเครือข่ายไร้สายต่าง ๆ อาจได้รับผลกระทบโดยตรง รวมถึงยังสามารถเป็นต้นตอของผลกระทบไปยังอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ของผู้อื่นด้วยเช่นกัน โดยผู้ใช้เครือข่ายไร้สายอาจถูกโจมตีด้วยมัลแวร์ผ่านข้อบกพร่องของระบบปฏิบัติการ และถูกเปลี่ยนสถานะมาเป็นผู้โจมตีโดยการส่งต่อหรือแพร่กระจายมัลแวร์เหล่านี้ไปยังอุปกรณ์อื่นผ่านเครือข่ายไร้สาย หรือบลูทูธ นอกจากนี้การใช้เครือข่ายไร้สายยังเปิดโอกาสให้ผู้ไม่ประสงค์ดีดักจับข้อมูลสำคัญ หรือรหัสผ่านบนเครือข่ายไร้สายได้อีกด้วย

4. ภัยคุกคามที่เกิดจากการถูกโจมตีแบบเจาะจงเป้าหมาย

ภัยคุกคามที่เกิดการโจมตีแบบเจาะจงเป้าหมาย (Targeted Attack) ที่มาจากหลายประเทศมีมากขึ้น ผู้โจมตีหรือแฮกเกอร์ (Hackers) ในประเทศต่าง ๆ จะใช้การโจมตีแบบเจาะจงเป้าหมาย อย่างต่อเนื่อง สร้างความเสียหายให้แก่โครงสร้างพื้นฐาน สถาบันการเงิน และองค์กรอื่น ๆของภาครัฐ และภาคเอกชนในหลายประเทศ อาชญากรไซเบอร์เหล่านี้จะใช้มาตรการที่รวดเร็วและรุนแรงในการโจรกรรมข้อมูล ภัยคุกคามประเภทนี้จัดว่าเป็นภัยคุกคามที่กระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง

2.5.2. ประเภทของผู้คุกคามทางไซเบอร์

ผู้คุกคามทางไซเบอร์หรือกลุ่มบุคคลและ/หรือองค์กรที่มีความชำนาญในการปฏิบัติการภัยไซเบอร์สามารถแบ่งออกเป็น 5 กลุ่ม (นงรัตน์ สายเพชร, 2556) ดังนี้

1. ประเทศที่มีความประสงค์ร้าย

กลุ่มนี้ได้แก่ รัฐบาลของบางประเทศที่มุ่งโจมตีกลุ่มงานความมั่นคงหรือกองทัพ โดยมีจุดมุ่งหมายที่จะสร้างความเสียหายให้เกิดขึ้นกับประเทศเป้าหมาย ซึ่งอาจเป็นการก่อกวนเว็บไซต์ของหน่วยงานต่าง ๆ การจารกรรมข้อมูลสำคัญ รวมถึงการสร้างความเสียหายให้กับโครงสร้างพื้นฐานของประเทศเป้าหมาย

2. ผู้ก่อการร้าย

กลุ่มนี้ได้แก่ ผู้ก่อการร้ายหรือผู้ไม่หวังดีซึ่งมีจุดประสงค์ที่จะทำลายผลประโยชน์ของชาติเป้าหมาย กลุ่มผู้ก่อการร้ายเหลานี้ใช้ไซเบอร์เป็นช่องทางการสื่อสาร โดยจะสร้างแบบแผนเพื่อหาเงินทุน หรือเพื่อเผยแพร่แนวความคิดที่เป็นภัยต่อประเทศเป้าหมาย

3. สายลับภาคเอกชน/องค์กรอาชญากรรม

กลุ่มนี้ได้แก่ สายลับภาคเอกชน หรือองค์กรอาชญากรรมซึ่งมีการใช้ไซเบอร์เป็นช่องทางในการบุกรุก และโจมตีระบบ โดยมีเป้าหมายเพื่อจารกรรมข้อมูลสำคัญ รวมถึงทรัพย์สินจากองค์กรภาครัฐ และภาคเอกชนต่าง ๆ กลุ่มนี้อาจเป็นกลุ่มปฏิบัติการของหน่วยงานความมั่นคงของบางประเทศ หรืออาจเป็นเพียงอาชญากรที่ตองการนำข้อมูลสำคัญไปหารายได้

4. แฮกเกอร์

กลุ่มแฮกเกอร์ (hackers) คือ กลุ่มผู้ที่พยายามหาช่องโหว่ของระบบ ลักลอบเจาะเข้าสู่ระบบเพื่ออ่านข้อมูลข่าวสาร เพื่อขโมย หรือเพื่อทำลายข้อมูลข่าวสารสำคัญเหล่านั้น ซึ่งจะทำให้เกิดความเสียหายแก่องค์กรเป้าหมาย แฮกเกอร์สามารถมาได้จากประเทศต่าง ๆ ทั่วโลก การป้องกันหรือ การสืบหาตัวผู้กระทำความผิดค่อนข้างทำได้ยาก

5. แฮกทิวิส

กลุ่มแฮกทิวิส (hacktivists) คือ กลุ่มแฮกเกอร์ที่มีแรงจูงใจทางการเมือง เป็นกลุ่มที่ต้องการผลักดันให้เกิดความเปลี่ยนแปลงทางการเมือง กลุ่มนี้มุ่งเน้นที่จะนำเสนอแนวคิดผ่านทางไซเบอร์และสร้างมูลเหตุที่ส่งผลต่อการเมืองและสังคมมากกว่าการสร้างความเสียหายให้กับโครงสร้างพื้นฐาน

2.5.3 ประเภทของภัยคุกคามทางไซเบอร์

หน่วยงาน The European Computer Security Incident Response Team (eCSIRT) ซึ่งเป็นเครือข่ายความร่วมมือของหน่วยงาน CSIRT ในสหภาพยุโรปได้จำแนกตามประเภทของภัยคุกคามทางไซเบอร์ออกเป็น 10 ประเภท ดังนี้

1. บอตเน็ต (Botnet) คือ โปรแกรมไม่พึงประสงค์ติดตั้งอยู่ในคอมพิวเตอร์ซึ่งสามารถโจมตีได้โดยอัตโนมัติหรือรับคำสั่งจากผู้ควบคุมผ่านเครือข่ายอินเทอร์เน็ตได้จากระยะไกล

2. สแปม (Spam) คือ การส่งจดหมายอิเล็กทรอนิกส์ออกไปยังผู้รับจำนวนมาก โดยผู้ที่ได้รับจดหมายเหลานั้น ไม่ได้มีความประสงค์ที่จะได้รับ ส่วนมากเป็นการโฆษณาสินค้าและบริการ

3. โอเพ่นดีเอ็นเอสรีโซลเวอร์ (Open DNS Resolver) คือ การตั้งค่าเครื่องให้บริการดีเอ็นเอส (DNS) อย่างไม่เหมาะสม ทำให้ผู้อื่นสามารถส่งข้อมูลโดเมนเนมหลอกลวงให้กับเครื่องบริการดีเอ็นเอส เพื่อใช้หลอกลวงผู้ใช้งาน

4. บรูตฟอร์ซ (Brute Force) คือ โปรแกรมที่เจาะระบบเป้าหมายด้วยวิธีการสุ่มข้อมูลตามอัลกอริทึมที่ผู้โจมตีคิดค้น เพื่อให้ได้ข้อมูลสำคัญหรือข้อมูลลับของระบบเป้าหมาย เช่น บัญชีชื่อผู้ใช้งานและรหัสผ่าน

5. มัลแวร์ยูอาร์แอล (Malware URL) คือ การที่ผู้ไม่ประสงค์ดีบุกรุกเข้าไปยังเว็บไซต์ของผู้อื่น และใช้พื้นที่ของเว็บไซต์นั้นในการเผยแพรโปรแกรมไม่พึงประสงค์

6. สแกนนิ่ง (Scanning) คือ การตรวจสอบข้อมูลของบริการของเครื่องแม่ข่ายโดยใช้วิธีส่งข้อมูลไปสู่ระบบที่เป็นเป้าหมาย และรวบรวมข้อมูลที่ได้จากการสแกนนิ่ง เพื่อใช้เป็นข้อมูลในการเจาะระบบ

7. โอเพ่นพร็อกซี่เซิร์ฟเวอร์ (Open Proxy Server) คือ การตั้งค่าบริการเว็บพร็อกซี่ (web proxy) ไม่เหมาะสมที่ยินยอมให้ผู้ใช้งานทั่วไปเรียกใช้งาน เพื่อเข้าถึงบริการเว็บในเครือข่ายอินเทอร์เน็ตได้โดยไม่มีระบบยืนยันตัวตน (authentication)

8. ฟิชชิ่ง (Phishing) คือ เว็บไซต์ปลอมที่ต้องการหลอกลวงเพื่อขโมยข้อมูลสำคัญของผู้ใช้งาน เช่น บัญชีผู้ใช้หรือรหัสผ่าน เป็นต้น

9. สตอร์มเวิร์ม (Storm Worm) คือ โปรแกรมไม่พึงประสงค์ในลักษณะเวิร์ม (Worm) ซึ่งสามารถแพร่กระจายได้ด้วยตัวเอง สตอร์มเวิร์มมีลักษณะการทำงานในรูปแบบบอตเน็ตต่างกันที่บอตเน็ตทั่วไปมีโครงสร้างการทำงานที่มีเครื่องที่ทำหน้าที่ควบคุม

10. ดีดอส (DDoS) คือ โปรแกรมที่โจมตีสภาพความพรอมใช้งานของระบบเพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้

2.5.4 ลักษณะและผลของภัยคุกคามทางไซเบอร์

เอกสาร Cybersecurity Articles ของไทยเซิร์ต ได้จำแนกลักษณะและผลของภัยคุกคามทางไซเบอร์ไว้ 8 ด้าน ดังนี้

1. เนื้อหาที่เป็นภัยคุกคาม (Abusive Content) เป็นการใช้ข้อมูล หรือเผยแพร่ข้อมูลที่ไม่เป็นจริง หรือไม่เหมาะสม เพื่อทำลายความน่าเชื่อถือของบุคคลหรือสถาบัน เพื่อก่อให้เกิดความไม่สงบหรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย การหมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่าง ๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้น ๆ

2. การโจมตีความสภาพพร้อมใช้งานของระบบ (Availability) เป็นการโจมตีเพื่อสร้างความเสียหายให้แก่ระบบให้บริการต่าง ๆ เช่น ทำให้เกิดความล่าช้า จนถึงขั้นที่ระบบไม่สามารถให้บริการต่อไปได้อาจเป็นการโจมตีระบบโดยตรง เช่น การโจมตีประเภท DoS (Denial of Service) หรือ เป็นการโจมตีโครงสร้างพื้นฐาน เช่น การให้บริการระบบไฟฟ้า น้ำประปา หรือระบบโทรศัพท์

3. การฉ้อฉล ฉ้อโกง หรือหลอกลวง เพื่อผลประโยชน์ (Fraud) เป็นความพยายามที่จะหาผลประโยชน์ด้วยการฉ้อโกง หรือหลอกลวง สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบ หรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาต เพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้า หรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์

4. ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) เป็นความพยายามในการรวบรวมข้อมูลระบบของผู้ไม่ประสงค์ดีด้วยการเรียกใช้บริการต่าง ๆ ที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน ชื่ออีเมล รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (Sniffing) และการล่อลวงต่าง ๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ

5. การเจาะระบบได้สำเร็จ (Intrusions) เป็นความพยายามที่สามารถเจาะเข้าระบบได้สำเร็จ และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต

6. ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts) เป็นความพยายามจะเจาะเข้าระบบผ่านจุดอ่อน หรือช่องโหว่ที่เป็นที่รู้จักในสาธารณะ (Common Vulnerabilities and Exposures: CVE) หรือผ่านจุดออนหรือช่องโหว่ใหม่ที่ยังไม่เคยพบมาก่อน เพื่อการเข้าครอบครอง

หรือทำให้เกิดความขัดข้องกับบริการต่าง ๆ ของระบบ รวมถึงความพยายามจะเจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน ด้วยวิธีการสุ่มข้อมูล หรือวิธีการทดสอบรหัสผ่านทุกค่า (Brute Force)

7. โค้ดมุ่งร้าย (malicious code or malware) คือ โค้ดมุ่งร้ายหรือเป็นอันตรายต่อระบบ ขโมยข้อมูล และ/หรือยังส่งต่อไปยังเครื่องผู้อื่น ตัวอย่างโปรแกรมในกลุ่มนี้ได้แก่ Virus, Worm, Trojan, Botnet, Horse, Spyware หรือ Web Scripts เป็นตน

8. การเข้าถึง/เปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต (Information Security) เป็นภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorized Access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized Modification) ได้

2.6 แนวคิดด้านวัฒนธรรม

คำว่า “วัฒนธรรม”เป็นคำไทยที่มาจากภาษาบาลีสันสกฤต แปลว่าธรรมเป็นเหตุ ให้เจริญ ตามหลักฐานว่า คำว่าวัฒนธรรมใช้เป็นครั้งแรก พ.ศ. 2483 ด้วยมีประกาศใช้พระราชบัญญัติบำรุงวัฒนธรรมแห่งชาติ พุทธศักราช 2483 กับฉบับที่ 2 เมื่อพุทธศักราช 2485 และเพื่อความเหมาะสมยิ่งขึ้น จึงได้ประกาศให้ใช้พระราชบัญญัติวัฒนธรรมแห่งชาติ พุทธศักราช 2486 ขึ้นใหม่ พจนานุกรมราชบัณฑิต พ.ศ. 2525 ให้ความหมายว่า สิ่งที่ทำให้เจริญงอกงามแก่หมู่คณะ, วิถีชีวิตของหมู่คณะ และมีความหมายที่นักวิชาการเป็นผู้กำหนดไว้หลายท่าน เช่น วัฒนธรรม หมายถึง ธรรมอันเป็นความเจริญ ซึ่งเป็นวิถีหรือทางดำเนินแห่งชีวิตของชุมชนหมู่หนึ่ง ซึ่งอยู่รวมกันในที่หนึ่ง หรือประเทศหนึ่งโดยเฉพาะประเพณี ศิลปะวรรณคดี ศาสนา (พระยาอนุมานราชธน, 2515) วัฒนธรรม คือ รูปแบบพฤติกรรม วิถีชีวิตและระบบสัญลักษณ์ที่มนุษย์สร้างขึ้นเพื่อใช้ในสังคม วัฒนธรรมในแต่ละสังคม เกิดจากการสั่งสมประสบการณ์และถ่ายทอดสู่รุ่นต่อรุ่นในสังคม โดยมีทั้งวัฒนธรรมในเชิงนามธรรมซึ่งได้แก่ ภาษา ความเชื่อ กริยามารยาท และวัฒนธรรมในเชิงรูปธรรมซึ่งได้แก่ อาคารบ้านเรือน วัด และศิลปกรรมประติมากรรมต่าง ๆ ตลอดจนสิ่งของเครื่องใช้ (อมรา พงศาพิชญ์, 2534)

สำนักงานคณะกรรมการวัฒนธรรมแห่งชาติ (2538) ได้ระบุว่า วัฒนธรรมในความหมายของคนไทยหมายถึง ความดีขึ้น ประณีตขึ้นกว่าเดิม โดยการศึกษา ฝึกหัด พร้อมการฝึกหัดหรือการทำให้ประณีตขึ้นซึ่งจิตใจ รสนิยม และจริตอัธยาศัยสภาพแห่งการที่ได้รับการอบรมหรือทำให้ประณีตขึ้น การบัญญัติคำว่าวัฒนธรรมขึ้นมานอกจากเพื่อตั้งสถาบันสำหรับการส่งเสริมเรื่องนี้เป็นการเฉพาะแล้ว ยังมุ่งหมายให้เป็นคำเทียบคำว่า Culture ในภาษาอังกฤษเช่นเดียวกับคำอื่น ๆ ที่ปรากฏในภาษาอังกฤษอันเป็นการบัญญัติคำใหม่ขึ้นในภาษาไทย ทั้งนี้มิได้หมายความว่าก่อนหน้าที่จะมีการบัญญัติคำนี้ขึ้นมาชาติไทยไม่มีวัฒนธรรม หรือไม่รู้จักวัฒนธรรม แท้จริงวัฒนธรรมมีมาแต่อดีตกาล แต่ไม่ได้ตั้งชื่อหรือคำศัพท์เฉพาะเรียกอย่างนี้ก่อนนั้น โดยอาจเรียกแยกตามส่วนต่าง ๆ ของวัฒนธรรม

ว่า ความเคยชินบ้าง ขนบธรรมเนียมบ้าง ประเพณีบ้าง จรรยามารยาทบ้าง และยังมีคำอื่น ๆ อีก สุดแล้วแต่เราจะพูดส่วนไหนของวัฒนธรรม แต่เมื่อบัญญัติคำว่าวัฒนธรรมขึ้นแล้ว คำนี้ก็มีความหมายรวมถึงเรื่องต่าง ๆ ที่กล่าวมาแล้วทั้งหมด

เสาวนีย์ จิตต์หมวด (2538) อธิบายว่า วัฒนธรรมคือวิถีการดำเนินชีวิต (Way of life) หรือรูปแบบแห่งพฤติกรรม (Behavior patterns) และบรรยายผลงานทั้งมวลที่มนุษย์ได้สร้างสรรค์ขึ้น อันได้แก่ ศาสนา ปรัชญา ภาษา กฎหมาย การปกครอง ศิลปะวิทยาการ เครื่องใช้ต่าง ๆ ฯลฯ ซึ่งมีการส่งต่อและสืบทอดติดต่อกันมา

ธิดารัตน์ รักประยูร (2545) อธิบายว่าวัฒนธรรมเป็นรากฐานจากผลผลิตและพื้นฐานการปรับตัวของมนุษย์และสิ่งแวดล้อมที่มีการสั่งสมประสบการณ์ของคนหลายชั่วอายุซึ่งในขณะเดียวกันวัฒนธรรมก็ได้รับใช้ขั้นตอนการดำรงชีวิตของมนุษย์ด้วย วัฒนธรรมนั้นเป็นสิ่งที่มนุษย์สร้างขึ้นและต้องเปลี่ยนแปลงไป เช่น วัฒนธรรมการแต่งกายวัฒนธรรมการบริโภคและวัฒนธรรมด้านภาษา เป็นต้น

ธีรยุทธ์ บุญมี (2546) อธิบายว่า วัฒนธรรมมีรากมาจากคำภาษาลาตินว่า Cultivare ซึ่งหมายถึง การไถพรวนแผ่นดิน จึงหมายถึงการบ่มเพาะ ประณีต ดีงาม อุดมสมบูรณ์การทำให้เสร็จสมบูรณ์ วัฒนธรรมในความหมายเชิงมานุษยวิทยาจึงหมายถึงแบบแผนชีวิตร่วมของคนชาติต่าง ๆ วัฒนธรรมเฉพาะของกลุ่มต่างๆ รวมความถึงความคิดแบบแผน ประเพณีพิธีกรรมต่างๆ ทุกอย่าง

พฤทธิสาณ ชุมพล (2548) อธิบายว่า วัฒนธรรม หมายถึง แบบอย่างของการดำรงชีวิตของชนหมู่ใดหมู่หนึ่ง และก่อนที่จะเป็นแบบอย่างขึ้นมาได้ จะต้องมีการปฏิบัติในหมู่คนจำนวนมากจนปฏิบัติตามกันไปทั้งกลุ่ม มีระยะเวลานานและเป็นแบบอย่างที่ชัดเจนแน่นอน

ฉัตรทิพย์ นาถสุภา และวันวร จะนู (2555) อธิบายว่า วัฒนธรรมหมายถึงความเชื่อคุณค่า ค่านิยม อุดมการณ์ และโลกทัศน์ คือโครงสร้างส่วนบนของสังคม เป็นสิ่งที่ผลักดันเป็นเหตุผลเบื้องหลังการกระทำ

จากคำอธิบายดังกล่าวข้างต้น วัฒนธรรมจึงหมายถึงวิถีในการดำเนินชีวิตที่มนุษย์สร้างขึ้น มีการถ่ายทอดจากคนรุ่นหนึ่งสู่คนอีกรุ่นหนึ่ง และอาจจะมีการเปลี่ยนแปลงได้

2.7 แนวคิดเกี่ยวกับวัฒนธรรมองค์กร (Organizational Culture)

“วัฒนธรรม” มักจะเชื่อมโยงกับพฤติกรรมองค์กร กระบวนการทำงานในองค์กร หรือ ความเป็นผู้นำในองค์กร จะเห็นได้ว่าวัฒนธรรมมิได้หมายรวมถึงทุก ๆ อย่างที่เกิดขึ้นในองค์กรในอดีต มีการแปลความหมายของคำว่าวัฒนธรรมออกมาอย่างมากมาย ขึ้นอยู่กับมุมมองของแต่ละบุคคลว่าจะมองในรูปแบบใด เช่น นักมานุษยวิทยาอาจมองว่า วัฒนธรรมเป็นขนบธรรมเนียมประเพณีที่มีการปฏิบัติสืบต่อกันมา ภายในกลุ่มชนกลุ่มหนึ่ง นักสังคมวิทยา อาจมองว่าเป็นความเชื่อ ค่านิยม และบรรทัด

ฐานของสังคมหนึ่ง ๆ ที่มีผลต่อการกำหนดพฤติกรรมของสมาชิกในสังคม ส่วนนักบริหารและจัดการอาจมองว่า วัฒนธรรม คือ กลยุทธ์ ลักษณะโครงสร้างขององค์กร และการควบคุมภายในองค์กร ในโลกปัจจุบัน มีความจำเป็นที่จะต้องเรียนรู้ถึงเทคโนโลยีต่าง ๆ สิ่งแวดล้อมที่ได้เปลี่ยนแปลงไป องค์กรต่าง ๆ ต้องมีการพัฒนาความสามารถของตนเพื่อรองรับการเปลี่ยนแปลงที่เกิดขึ้น โดยที่ทุกคนในองค์กรต้องมีความ กระตือรือร้น ในการหาวิธีการ ที่จะมาปรับเปลี่ยนในการพัฒนาการทำงานของตน ตลอดจนพฤติกรรมที่คนในองค์กรยึดถือ เพื่อเป็นแนวทางในการปฏิบัติงาน ซึ่งแบบแผนพฤติกรรมที่บุคคลในองค์กรยึดถือ เป็นแนวทางในการประพฤติปฏิบัติ ที่มีพื้นฐานมาจากความเชื่อ ค่านิยม นั่นก็ คือ วัฒนธรรมองค์กร (พร รัตน์ รัตนศิริวงศ์, ม.ป.ป)

2.7.1 ความหมายของวัฒนธรรมองค์กร

วัฒนธรรมองค์กร คือ ระบบของสิ่งที่ก่อให้เกิดความเข้าใจกันในแนวทางการประพฤติและแนวทางในการทำงานและความสัมพันธ์ (Glue) ในองค์กรนั้นๆ ซึ่งสามารถชี้ได้ว่าวัฒนธรรมองค์กรตามความหมายที่มีการศึกษาผลในการวางแผนการบริหาร (Management) องค์กรโดยตรง เป็นสิ่งที่กำหนดทิศทางในการวางกลยุทธ์ (Strategy) และรวมไปถึงเป็นแนวโน้มในการสร้างวิสัยทัศน์ (Vision) ขององค์กรนั้น ๆ ซึ่งเป็นแนวทางที่องค์กรใช้เป็นหลักในการสร้างองค์กรให้ประสบความสำเร็จ (วรวุฒิ กิจสิริศาล, 2553)

ฉันทนา (2550) กล่าวไว้ว่า ความหมายของวัฒนธรรมองค์กร สามารถแบ่งพิจารณาได้ดังนี้

1) วัฒนธรรม (Culture) หมายถึงกลุ่มของค่านิยม ความเข้าใจ ความเชื่อ และมาตรฐานที่สมาชิกในองค์กรยึดถือร่วมกัน

2) วัฒนธรรมองค์กร (Organizational Culture) หมายถึง ระบบการยึดถือในสิ่งที่มีความหมายร่วมกันของสมาชิกภายในองค์กรซึ่งมีอิทธิพลต่อการปฏิบัติงาน การตัดสินใจ และพฤติกรรมอื่น ๆ

ดังนั้นวัฒนธรรมองค์กรจึงเป็นฐานคิด เป็นเป้าหมาย เป็นเครื่องมือที่บอกให้สมาชิกในองค์กรทราบ ว่าการกระทำแบบใดดีหรือไม่ดี เป็นทิศทางในการตัดสินใจ และหลอมรวมสมาชิกในองค์กรโดยการใช้ภาษาเดียวกัน การกำหนดการเป็นคนในและคนนอกองค์กร กำหนดอำนาจและพัฒนาแนวคิด หรือบรรทัดฐานความคิดที่กำหนดความสัมพันธ์ในกลุ่มนั้น กำหนดการให้รางวัลและการลงโทษเพื่อให้สมาชิกมีทิศทางเดียวกัน และอธิบายสิ่งที่ไม่เข้าใจให้เข้าใจได้

สมคิด (2548) ได้ให้ความหมายวัฒนธรรมองค์การไว้ว่า หมายถึง ความคิด ความเชื่อ แผนปฏิบัติงาน และการดำรงชีวิตของบุคลากรในองค์การหนึ่ง ๆ ซึ่งบุคลากรส่วนใหญ่ขององค์การยอมรับและปฏิบัติเป็นประเพณีและใช้เป็นแบบแผนในการปฏิบัติตนในฐานะสมาชิกขององค์การ

สุนทร (2540) ได้รวบรวมความหมายของวัฒนธรรมองค์การจากนักวิชาการหลายท่านนำมาจัดเป็นกลุ่มได้ 7 กลุ่ม ดังนี้

1. วัฒนธรรมองค์การ หมายถึง กฎเกณฑ์ที่ไม่เป็นทางการ (Implicit Rules) ในหน่วยงานกฎเกณฑ์ดังกล่าวเป็นสิ่งที่พนักงานใหม่ต้องเรียนรู้เพื่อที่จะสามารถทำงานในหน่วยงานนั้นได้

2. วัฒนธรรมองค์การ หมายถึง พฤติกรรมที่ปฏิบัติกันอย่างสม่ำเสมอขณะที่บุคคลติดต่อเกี่ยวข้องกับผู้อื่น เช่น พิธีการต่าง ๆ ในหน่วยงาน ธรรมเนียมหรือแนวทางการปฏิบัติในองค์การงานฉลองในโอกาสต่าง ๆ ของหน่วยงาน

3. วัฒนธรรมองค์การ หมายถึง ความรู้ ความคิด ความเชื่อ ข้อสมมติฐาน (Basic Assumption) และค่านิยมที่มีอยู่ร่วมกันภายในจิตใจของคนจำนวนหนึ่ง หรือคนส่วนใหญ่ในองค์การ คนกลุ่มใหญ่ดังกล่าวใช้ระบบความรู้ความคิดร่วมกันนี้เป็นแนวทางในการคิดตัดสินใจและทำความเข้าใจสภาพแวดล้อมภายในองค์การ

4. วัฒนธรรมองค์การ หมายถึง ความหมายของเหตุการณ์และพฤติกรรมต่าง ๆ ภายในหน่วยงานที่สมาชิกองค์การจำนวนหนึ่งหรือส่วนใหญ่เข้าใจร่วมกัน หรืออาจกล่าวอีกนัยหนึ่งว่าเป็นความเข้าใจร่วมกันของคนจำนวนหนึ่งหรือส่วนใหญ่ภายในหน่วยงานที่มีต่อเรื่องราวทั้งหลายในองค์การ

5. วัฒนธรรมองค์การ หมายถึง บรรทัดฐานของกลุ่ม (Group Norms) ซึ่งหมายถึงมาตรฐาน (Standard) ของพฤติกรรมที่กลุ่มคาดหวังหรือสนับสนุนให้สมาชิกในกลุ่มปฏิบัติตามคาดว่าความคิดนี้อาจจะได้รับอิทธิพลจากทฤษฎีกระบวนการกลุ่ม (Group Process) ซึ่งสนใจโครงสร้างกระบวนการ และประสิทธิผลของกลุ่มจึงนำความคิดเกี่ยวกับบรรทัดฐานของกลุ่มมาเป็นหัวใจของวัฒนธรรมองค์การ

6. วัฒนธรรมองค์การ หมายถึง สิ่งประดิษฐ์(Artifacts) ภายในหน่วยงาน สิ่งประดิษฐ์ภายในหน่วยงานอาจเป็นรูปร่างของอาคาร ลักษณะของเฟอร์นิเจอร์และการตกแต่ง การวางผังโต๊ะทำงาน ตราของหน่วยงาน (Organizational Logo) ฯลฯ นักวิชาการในแนวนี้เชื่อว่าสิ่งประดิษฐ์ต่าง ๆ ดังกล่าวสามารถสะท้อนให้เห็นถึงวัฒนธรรมของหน่วยงาน รวมถึงสะท้อนภาพพจน์ของหน่วยงานต่อสาธารณชนด้วย

7. วัฒนธรรมองค์การ หมายถึง สิ่งต่าง ๆ อันประกอบด้วยสิ่งประดิษฐ์ แบบแผนพฤติกรรมบรรทัดฐาน ความเชื่อ ค่านิยม อุดมการณ์ความเข้าใจ และข้อสมมุติพื้นฐานของคนจำนวนหนึ่งหรือส่วนใหญ่ในองค์การ การนิยามวัฒนธรรมองค์การในลักษณะนี้เป็น การรวมความหมายของวัฒนธรรมองค์การหลายความหมายที่กล่าวมาข้างต้นเข้าด้วยกัน เป็นการนิยามในลักษณะที่ว่าวัฒนธรรมองค์การประกอบด้วยองค์ประกอบต่าง ๆ (Element) หลายองค์ประกอบเข้าด้วยกัน

2.7.2 หน้าที่ของวัฒนธรรมองค์กร

Gutknecht (1982 อ้างถึงใน กริช, 2538) กล่าวไว้ว่าวัฒนธรรมองค์การมีหน้าที่ 3 ประการ คือ

1. เป็นเกณฑ์ในการสร้างกฎ ข้อบังคับ วัฒนธรรมช่วยสร้างให้สมาชิกมีกฎทางสังคมในการตีความหรือแสดงพฤติกรรมในการแก้ปัญหาที่เกี่ยวข้อง

2. เป็นสิ่งกระตุ้น วัฒนธรรมช่วยให้สมาชิกมีศรัทธา เป็นแรงจูงใจให้แต่ละคนปรับลักษณะเฉพาะของตนให้มีบทบาท ค่านิยม ฯลฯ ที่สอดคล้องกับวัฒนธรรมองค์การ

3. เป็นเครื่องมือผนึกกำลัง วัฒนธรรมช่วยให้สมาชิกผสมผสานติดต่อสมาคมกันและร่วมมือกัน ช่วยให้องค์การบรรลุเป้าหมาย

2.7.3 ประเภทของวัฒนธรรมองค์กร

2.7.3.1 วัฒนธรรมลักษณะสร้างสรรค์ (The Constructive Culture)

วัฒนธรรมองค์กรลักษณะสร้างสรรค์ตามแนวคิดของ Cooke and Lafferty, 1989 (อ้างถึงใน จารุวรรณ ประดา, 2545) เป็นองค์กรที่มีลักษณะของการให้ความสำคัญกับค่านิยมในการทำงาน โดยมุ่งส่งเสริมให้สมาชิกในองค์กรมีปฏิสัมพันธ์และสนับสนุนช่วยเหลือซึ่งกันและกัน ทำงานมีลักษณะที่ส่งผลให้สมาชิกภายในองค์กรประสบความสำเร็จในการทำงาน และมุ่งที่ความพึงพอใจของบุคคลเกี่ยวกับความต้องการความสำเร็จในการทำงาน และมุ่งที่ความพึงพอใจของบุคคลเกี่ยวกับความต้องการความสำเร็จ และความต้องการไมตรีสัมพันธ์ ซึ่งลักษณะพื้นฐานของวัฒนธรรมองค์กรเชิงสร้างสรรค์ แบ่งเป็น 4 มิติ คือ

1) มิติมุ่งความสำเร็จ (Achievement) คือ องค์กรที่มีค่านิยม และพฤติกรรมการแสดงออกในการทำงานของสมาชิกภายในองค์กรที่มีภาพรวมของลักษณะการทำงานที่ดี มีการตั้งเป้าหมายร่วมกัน พฤติกรรมการทำงานของทุกคนเป็นแบบมีเหตุมีผล มีหลักการ และการวางแผนที่มีประสิทธิภาพ มีความกระตือรือร้น และมีความสุขในการทำงาน รู้สึกว่างานมีความหมาย และมีความท้าทาย ลักษณะเด่นคือ สมาชิกในองค์กรมีความกระตือรือร้น และรู้สึกว่างานท้าทายความสามารถอยู่ตลอดเวลา

2) มิติมุ่งสัจการแห่งตน (Self- Actualizing) คือ องค์กรที่มีค่านิยม และพฤติกรรม การแสดงออกของการทำงานในทางสร้างสรรค์ โดยเน้นความต้องการของสมาชิกในองค์กรตามความ คาดหวัง เป้าหมายการทำงานอยู่ที่คุณภาพงานมากกว่าปริมาณงานโดยที่เป้าหมายของตนสอดคล้องกับเป้าหมายขององค์กร รวมทั้งความสำเร็จของงานมาพร้อม ๆ กับความก้าวหน้าของสมาชิกในองค์กร ทุกคนมีความเต็มใจในการทำงาน และภูมิใจในงานของตน สมาชิกทุกคนได้รับการสนับสนุนในการพัฒนาตนเองจากงานที่ทำอยู่ รวมทั้งมีความอิสระในการพัฒนางานของตน

ลักษณะเด่น คือ สมาชิกในองค์กร มีความยึดมั่นผูกพันกับงาน และมีบุคลิกภาพที่มีความพร้อมในการทำงานสูง

3) มิติมุ่งบุคคล (Humanistic - Encouraging) คือ องค์กรที่มีค่านิยมและพฤติกรรม การแสดงออกของการทำงานที่มีรูปแบบการบริหารจัดการแบบมีส่วนร่วมและมุ่งบุคคลเป็นศูนย์กลาง ให้ความสำคัญกับสมาชิกในองค์กร โดยถือว่าสมาชิกคือ ทรัพยากรที่มีค่าที่สุดขององค์กร การทำงานมีลักษณะติดต่อสื่อสารที่มีประสิทธิภาพ สมาชิกมีความสุข และภูมิใจในการทำงาน มีความสุขต่อการสอน การนิเทศงานและการเป็นพี่เลี้ยงให้แก่กัน ทุกคนในองค์กรได้รับการสนับสนุนความก้าวหน้าในการทำงานอย่างสม่ำเสมอ ลักษณะเด่น คือ ทรัพยากรบุคคลเป็นสิ่งสำคัญที่สุดขององค์กร

4) มิติมุ่งไมตรีสัมพันธ์ (Affiliate) คือ องค์กรที่มีลักษณะที่มุ่งให้ความสำคัญกับสัมพันธภาพระหว่างบุคคล สมาชิกทุกคนในองค์กรมีความเป็นกันเอง เปิดเผย จริงใจ และไวต่อความรู้สึกของเพื่อนร่วมงานและเพื่อนร่วมทีม ได้รับการยอมรับ และเข้าใจความรู้สึกซึ่งกันและกัน ลักษณะเด่น คือ ความเป็นเพื่อนและความจริงใจต่อกัน

ดังนั้น วัฒนธรรมลักษณะสร้างสรรค์จะเน้นการทำงานอย่างสร้างสรรค์ สร้างค่านิยมในการทำงานที่มุ่งความสำเร็จและความพึงพอใจในการทำงานของผู้ปฏิบัติงาน มีความ กระตือรือร้นในการทำงาน เน้นการทำงานเป็นทีม สัมพันธภาพระหว่างผู้ร่วมงาน และมีความรู้สึกว่างานท้าทายความสามารถอยู่ตลอดเวลา ต่อไปก็จะขอกล่าวถึงวัฒนธรรมองค์กรแห่งการเรียนรู้ซึ่งเป็นวัฒนธรรมองค์กรอีกรูปแบบหนึ่งที่มีความสำคัญที่จะทำให้บุคลากรในองค์กรเกิดการพัฒนาในการ เรียนรู้การทำงานร่วมกันจนบรรลุเป้าหมายขององค์กร

2.7.3.2 วัฒนธรรมองค์กรแห่งการเรียนรู้ (Learning Organization)

Peter Senge (1990) เชื่อว่าหัวใจของการสร้าง Learning Organization อยู่ที่การสร้างวินัย 5 ประการในรูปของการนำไปปฏิบัติของบุคคล ทีม และองค์กรอย่างต่อเนื่อง วินัย 5 ประการ ที่เป็นแนวทางสนับสนุนการปฏิบัติ เพื่อสร้างกระบวนการเรียนรู้ทั้งองค์กรมีดังนี้

1) Personal Mastery : มุ่งสู่ความเป็นเลิศ และรอบรู้โดยมุ่งมั่นที่จะพัฒนาตนเองให้ไปถึงเป้าหมาย ด้วยการสร้างวิสัยทัศน์ส่วนตน (Personal Vision) เมื่อลงมือกระทำและต้องมุ่งมั่นสร้างสรรค์จึงจำเป็นต้องมีแรงมุ่งมั่นใฝ่ดี (Creative Tended) มีการใช้ข้อมูลข้อเท็จจริงเพื่อคิด วิเคราะห์ และตัดสินใจ (Commitment to the Truth) ที่ทำให้มีระบบการคิดตัดสินใจที่ดี รวมทั้งใช้การฝึกจิตใต้สำนึกในการทำงาน (Using Subconsciousness) ด้วยการดำเนินไปอย่างอัตโนมัติ

2) Mental Model มีรูปแบบวิธีการคิดและมุมมองที่เปิดกว้าง ผลลัพธ์ที่จะเกิดจากรูปแบบแนวคิดนี้จะออกมาในรูปของผลลัพธ์ 3 ลักษณะคือ เจตคติ หมายถึง ท่าทีหรือ

ความรู้สึกของบุคคลต่อสิ่งใดสิ่งหนึ่ง เหตุการณ์หรือเรื่องราวใด ๆ ทัศนคติแนวความคิดเห็นและกระบวนทัศน์ กรอบความคิด แนวปฏิบัติที่เราปฏิบัติตาม ๆ กันไป จนกระทั่งกลายเป็นวัฒนธรรมขององค์กร

3) Shared Vision การสร้างและสานวิสัยทัศน์วิสัยทัศน์องค์กรเป็นความมุ่งหวังขององค์กรที่ทุกคนต้องร่วมกันบูรณาการให้เกิดเป็นรูปธรรมในอนาคต ลักษณะวิสัยทัศน์องค์กรที่ดีคือ กลุ่มผู้นำต้องเป็นฝ่ายเริ่มหันเข้าสู่กระบวนการพัฒนาวิสัยทัศน์อย่างจริงจัง วิสัยทัศน์นั้นจะต้องมีรายละเอียดชัดเจนเพียงพอที่จะนำไปเป็นแนวทางปฏิบัติได้ วิสัยทัศน์องค์กรต้องเป็นภาพบวกต่อองค์กร

4) Team Learning การเรียนรู้ร่วมกันเป็นทีม องค์การมุ่งเน้นให้ทุกคนในทีมมีสำนึกร่วมกันว่า เรากำลังทำอะไรและจะทำอะไรต่อไป ทำอย่างไรจะช่วยเพิ่มคุณค่าแก่ลูกค้า การเรียนรู้ร่วมกันเป็นทีมขึ้นกับ 2 ปัจจัย คือ IQ และ EQ ประสานกับการเรียนรู้ร่วมกันเป็นทีม และการสร้างภาวะผู้นำแก่ผู้นำองค์กรทุกระดับ

5) System Thinking มีความคิดความเข้าใจเชิงระบบ ทุกคนควรมีความสามารถในการเข้าใจถึงความสัมพันธ์ระหว่างสิ่งต่าง ๆ ที่เป็นองค์ประกอบสำคัญของระบบ นอกจากมองภาพรวมแล้ว ต้องมองรายละเอียดของส่วนประกอบย่อยในภาพนั้นให้ออกด้วย วินัยข้อนี้สามารถแก้ไขปัญหาที่สลับซับซ้อนต่าง ๆ ได้เป็นอย่างดีและการพัฒนาองค์กรให้เป็นองค์กรแห่งการเรียนรู้นั้นจะต้องมีการปรับเปลี่ยนวิธีการในการคิด และปฏิสัมพันธ์ของบุคลากรในองค์กร ความมุ่งมั่นหรือทุ่มเทของบุคลากร ในองค์กร การที่จะองค์กรก้าวสู่การเป็นองค์กรแห่งการเรียนรู้นั้น ซึ่งพสุ เดชะรินทร์, 2549 กล่าวว่า ประกอบด้วย

- Openness to Experience คือ การที่บุคคลในองค์กรมีการเปิดใจ หรือ ยอมรับต่อประสบการณ์ต่าง ๆ ทั้งประสบการณ์จากภายนอกและภายในองค์กร เนื่องจากปัญหาของหลาย ๆ องค์กร คือ ความไม่พร้อมหรือไม่อยากจะเรียนรู้

- Encourage of Responsible Risk – Taking ซึ่งวัฒนธรรมองค์กรจะต้องเอื้อให้บุคลากรในองค์กรพร้อมและยอมรับต่อความเสี่ยงในการทำสิ่งใหม่ ๆ เนื่องจากการที่เราริเริ่มหรือทำสิ่งใหม่ ๆ ที่ไม่เคยทำมาก่อน ก็จะทำให้เราเกิดการเรียนรู้เกิดขึ้น แต่ในขณะเดียวกันก็มีความเสี่ยงที่มากับสิ่งใหม่ ๆ นั้นด้วย ดังนั้น การยอมรับต่อความเสี่ยงที่เกิดขึ้นก็เป็นสิ่งที่สำคัญต่อการกระตุ้นให้เกิดการเรียนรู้

- ความกล้าที่จะยอมรับต่อความสำเร็จและล้มเหลว ทั้งนี้เนื่องจากการเรียนรู้ที่สำคัญคือ การเรียนรู้จากประสบการณ์ในอดีต ซึ่งประสบการณ์ในอดีตนั้นมีทั้งสำเร็จและ ล้มเหลว และถ้าเรายอมรับต่อความสำเร็จ และล้มเหลวได้เราก็พร้อมที่จะเรียนรู้จากความสำเร็จ และ ล้มเหลวที่เราได้ประสบมา

ดังนั้น การที่เป็นองค์กรแห่งการเรียนรู้นั้น บุคคลในองค์กรต้องมีการเปิดใจยอมรับ เรียนรู้ในสิ่งใหม่ๆ กล้าเผชิญกับความเสี่ยงในการทำสิ่งใหม่ๆ ที่เกิดขึ้นทั้งนี้เพื่อเป็นการกระตุ้นให้เกิดการเรียนรู้ สู่การเป็นองค์กรแห่งการเรียนรู้ ดังที่กล่าวมาแล้ว

2.7.3.3 วัฒนธรรมองค์กรอัจฉริยะ (Intelligence Culture)

วิจารณ์ พานิช (2550) กล่าวว่า เป็นองค์กรที่เน้นความรู้เป็นสิ่งสำคัญแต่การเรียนรู้และการสร้างความรู้สำคัญที่สุด ดังนั้นเป้าหมายขององค์กรนี้คือ สามารถในการเผชิญกับสภาพอนาคตที่ไม่แน่นอนได้และต้องมีขีดความสามารถ 12 ประการ ในการเป็นองค์กรอัจฉริยะ คือ

1) มีความมุ่งหมาย มุ่งมั่น ที่ชัดเจน การเป็นเบอร์ 1 ขององค์กรคือ ต้องมีการ Manage Share Vision ทุกคนในองค์กรร่วมคิดและเป็นเจ้าของเป้าหมาย แต่เป็นเป้าหมายในระดับคุณค่า มีความมุ่งมั่น (Passion) สิ่งเหล่านี้จะเกิดขึ้นได้ต้องมีกระบวนการ Build Shared Vision ต้องมีการ Manage และต้องมี Share Vision ร่วมกันทุกวัน

2) ตั้งอยู่ในความไม่ประมาท (อปมาโท มีสติ& ปัญญา) มีความเชื่อในความเปลี่ยนแปลง (ตั้งอยู่ในความไม่ประมาท) ต้องตั้งสติอยู่ในการเปลี่ยนแปลง ต้องทำ Change Management ทั้งภายในและภายนอก โดยต้องใช้การจัดการเชิงบวก (Positive Change Management)

3) มีและใช้แผนยุทธศาสตร์ KM (Knowledge Management) ต้องมีแผน KM เป็นส่วนหนึ่งของแผนยุทธศาสตร์องค์กร

4) มีและใช้ภาวะผู้นำและแกนนำ (Leadership) ผู้บริหารสูงสุดต้องบริหาร กระบวนทัศน์ ภาวะผู้นำต้องมีอยู่ทั่วทั้งองค์กร อยู่ในทุกคน ทุกคนเป็นผู้นำ นำการเปลี่ยนแปลง ณ จุดที่ตนเองรับผิดชอบ หาวิธีการใหม่ ๆ สร้างนวัตกรรม สร้างการเปลี่ยนแปลงกับเพื่อนร่วมงาน มีการทำ CQI (Continuous Quality Improvement) ร่วมกันสร้าง Organizational Knowledge จาก Individual Knowledge

5) จัดการความสัมพันธ์ระหว่างคน องค์กรอัจฉริยะเกิดจากความสัมพันธ์ระหว่างคน เพราะความสัมพันธ์ระหว่างคนจะทำให้องค์กรมีพลังมากขึ้น

6) ทักษะพื้นฐานของพนักงาน เป็นทักษะในระดับวิธีคิดและให้คุณค่าเป็นการปฏิบัติการคิด การแลกเปลี่ยนเรียนรู้ ทักษะที่สำคัญที่สุดคือทักษะการฟัง ทักษะในการเข้าใจ Mental Model ของตนเองและของผู้อื่น เป็นการพัฒนาองค์กร

7) ทักษะในการใช้ “ตัวช่วย” (Enablers) KM Enabler คือ เครื่องมือที่เป็นตัวช่วยให้เกิดการเรียนรู้อย่างมีพลัง ใช้เท่าที่จำเป็น ตัวอย่างตัวช่วย เช่น BAR (Before Action Review), OM (Outcome Mapping) เป็นต้น

8) ไร้กำแพง กำแพงไม่ใช่กำแพงจริงแต่เป็นกำแพงใจ ปฏิสัมพันธ์ระหว่างคนทำให้เกิดการเรียนรู้ อุปสรรคที่สำคัญคือต่างคนต่างอยู่เป็นหน่วย ไม่มีเวลามาพูดคุย การทำงานต้องไม่เริ่มจากศูนย์เพราะเพื่อนร่วมงานบางคนอาจมีความรู้นั้นอยู่แล้ว มีประสบการณ์ของเพื่อนมาช่วยแก้ปัญหา เครื่องมือทลายกำแพง เช่น CFT (Cross Function Team: กลุ่มของบุคลากรที่มาจากหลายหน่วยงาน ภายในองค์กรมีความรู้และทักษะหลากหลายมารวมกัน เพื่อวัตถุประสงค์ของการแก้ปัญหาเรื่องใดเรื่องหนึ่ง), Task Force คณะทำงานเฉพาะกิจ, Job Rotation ทำงานโดยหมุนความรู้ให้เพื่อนร่วมงานด้วย, CoP: Community of Practice เป็นเครือข่ายชุมชนแนวปฏิบัติเป็นเครื่องมือทรงพลังต่อการแลกเปลี่ยนเรียนรู้ประสบการณ์ในการปฏิบัติเรื่องใดเรื่องหนึ่งระหว่างสมาชิกชุมชน เป็นต้น

9) อิสรภาพ บรรยากาศเชิงบวก บางหน่วยงานมี Talent Management ต้องให้คนทำงานสามารถลองผิดลองถูกได้เองและทำให้คนทำงานได้เป็นผู้นำตัวเล็ก ๆ กล้าคิดที่จะเปลี่ยนวิธีการทำงานของตนอยู่ตลอดเวลา ทำให้คนทำงานมีความสุข

10) มีและใช้ การจัดการคนเก่ง การจัดการขุมทรัพย์ทางปัญญา หัวใจอยู่ที่การเสาะ Resources ซึ่งก็คือ ทรัพยากรทางปัญญา Intellectual Capital (IC) เป็นสิ่งที่จับต้องได้และไม่ได้ เช่น เป็นคน เป็นความสัมพันธ์ เป็นวัฒนธรรมเป็นความรู้ใหม่เป็นต้น

11) มีและใช้ ระบบบันทึก ขุม/คลังความรู้ในองค์กรต้องสนับสนุนให้คนทำงานจดบันทึก จดในสิ่งที่ตนสนใจขึ้นจากการทำงาน บันทึกการเรียนรู้จากหน้างาน แล้วนำมาทำความเข้าใจ ยกระดับความรู้ร่วมกัน และมีการจัดการเรื่องเล่าให้เป็นหมวดหมู่

12) มีและใช้ระบบ ICT (Information Communication Technology)
ดังนั้น องค์กรอัจฉริยะ คือ องค์กรที่มีความรู้ความสามารถมากกว่าปกติ CIA: Central Intelligence Agency เป็นองค์กรที่มีนักคิด นักวิเคราะห์ นักสืบค้น นักปฏิบัติทำงานอยู่ เป็นองค์กรที่มีฐานความรู้ ภูมิปัญญา ฉลาดคิด ฉลาดฟัง ฉลาดทำ ทั้งนี้ต้นกำเนิดขององค์กรอัจฉริยะเกิดมาจาก องค์ความรู้เดิมและองค์ความรู้ใหม่ทักษะและรูปแบบความคิด เกิดสารสนเทศใหม่ ก่อให้เกิดทางเลือกที่หลากหลาย ฉลาดเลือก และฉลาดทำ อันเป็นฐานของพลังความรู้ (Knowledge Power) ที่จะเป็นพลังแห่งความคิดสร้างสรรค์ เพื่อสู่การปฏิบัติ โดยมีความเป็นเลิศหรือเก่งจริงใน 3 ประการ คือ

- ความเป็นเลิศในวิชาการ (Academic Excellence) โดยอาศัยฐานความรู้ (Knowledge Base) ความรู้ที่สำคัญควรมาจากความรู้ความสามารถของบุคลากรในองค์กร โดยพัฒนาให้เป็นองค์กรแห่งการเรียนรู้ (Learning Organization) ทั้งนี้ ผู้บริหารหรือผู้นำจะ

เป็นผู้ทำหน้าที่เป็นผู้เชื่อมโยงเพื่อการถ่ายโอนทางสติปัญญา กล่าวคือ ลดช่องว่างการถ่ายโอนทางสติปัญญาของบุคลากรในองค์กร (Intelligence Transfer Gap: ITP) จัดให้มีการแลกเปลี่ยนความรู้กันให้มากที่สุด ก่อให้เกิดการประสานทั้งองค์ความรู้เดิม และองค์ความรู้ใหม่

- ความเป็นเลิศในวิชาชีพอย่างมืออาชีพ (Professional Excellence) บุคลากรในองค์กรจะต้องมีความเป็นมืออาชีพ นั้นคือ ผู้บริหารจะต้องเป็นผู้บริหารมืออาชีพ คือ จะต้องเก่งคิด เก่งคน และเก่งงาน บุคลากรในองค์กรปฏิบัติงานอย่างมืออาชีพ ถ้าเป็นครู ก็ต้องเป็นครูมืออาชีพ ทั้งนี้ จะต้องสร้างและพัฒนาบุคลากรในองค์กรให้เป็นผู้ปฏิบัติงาน มีการเรียนรู้งาน และรับผิดชอบงานอย่างมืออาชีพนั่นเอง

- ความเป็นเลิศในวิถีการดำเนินชีวิต (Life Excellence) โดยการให้ความสำคัญกับบุคคล เข้าใจในวิถีชีวิตและการดำเนินชีวิตของบุคลากรในองค์กรเป็นอย่างดีส่งเสริมให้บุคลากรดำเนินชีวิตได้อย่างมีความสุข

ฉะนั้น การบริหารองค์กรจึงต้องใช้ฐานของการบริหารการจัดการความรู้เพื่อให้เกิดเป็นองค์กรแห่งการเรียนรู้ถือเป็นการพัฒนาบุคลากรอย่างสมบูรณ์เป็นการบริหารภูมิปัญญาเพื่อเพิ่มพลังและศักยภาพอำนาจในการปฏิบัติของบุคลากรอย่างเต็มที่ สู่ความเป็นอัจฉริยะขององค์กร และยังมีวัฒนธรรมองค์กรที่มีความสำคัญต่อการเปลี่ยนแปลงจากวัฒนธรรมหนึ่งไปยังอีกวัฒนธรรมหนึ่ง

2.7.3.4 วัฒนธรรมองค์กรการเปลี่ยนแปลง

ในปัจจุบันนี้ความก้าวหน้าของโลกเทคโนโลยีต่างๆ สิ่งแวดล้อมที่ได้เปลี่ยนแปลงไป องค์กรต่าง ๆต้องมีการพัฒนาความสามารถของตนเพื่อรองรับการเปลี่ยนแปลงที่เกิดขึ้น ดังนั้นองค์กรที่ต้องรองรับการเปลี่ยนแปลง มีแนวทางดังนี้

1) เริ่มจากทำการวิเคราะห์สภาพวัฒนธรรมองค์กรที่เป็นอยู่ เพื่อให้เข้าใจในองค์ประกอบต่าง ๆ ที่ควรจะต้องมีการเปลี่ยนแปลง

2) ทำความเข้าใจกับผู้ปฏิบัติงาน เพื่อให้เห็นความจำเป็นที่ว่าองค์กรจะอยู่รอดไม่ได้หากไม่มีการเปลี่ยนแปลงเกิดขึ้น

3) แต่งตั้งผู้นำที่มีวิสัยทัศน์ใหม่ๆ เข้ามาทำหน้าที่ผลักดันการเปลี่ยนแปลง

4) ทำการปรับโครงสร้างและปรับองค์กรให้เหมาะสม

5) สร้างสื่อใหม่ ๆ ที่จะช่วยสื่อวิสัยทัศน์นั้นออกมาให้คนอื่นได้ทราบ

6) ปรับเปลี่ยนกระบวนการคัดเลือกและกระบวนการเรียนรู้ทางสังคม การประเมินผล และระบบรางวัลจูงใจที่จะช่วยสนับสนุนค่านิยม และปรัชญาใหม่ ๆ เพื่อสร้างวัฒนธรรมใหม่ให้เกิดขึ้น

องค์กรไม่สามารถเปลี่ยนแปลงได้โดยบุคคลใดบุคคลหนึ่ง หรือกลุ่มบุคคลใดกลุ่มบุคคลหนึ่ง แต่จะเปลี่ยนแปลงอย่างเงียบ ๆ โดยวัฒนธรรมในองค์กรอย่างมีระเบียบแบบแผน อย่างไรก็ตามการเปลี่ยนแปลงโครงสร้างภายในองค์กรหรือการบริหารงานถือเป็นอีกปัจจัยหนึ่งที่ส่งผลต่อการเปลี่ยนแปลงทางวัฒนธรรม ดังตัวอย่างเช่น องค์กรจะมีการเปลี่ยนแปลงแนวทางในการคัดเลือกบุคลากรหรือสวัสดิการสำหรับบุคลากร ก็จะกระทำอย่างค่อยเป็นค่อยไปเหมือนกับการเบนเป้าหมาย จนในที่สุดก็ได้รับการยอมรับในข้อตกลงต่าง ๆ ซึ่งเป็นธรรมชาติ จนเกิดเป็นวัฒนธรรมในองค์กร ในที่สุด ทิศทางการเปลี่ยนแปลงของวัฒนธรรมในองค์กรล้วนมาจากความคิดสร้างสรรค์ การต้องการความเปลี่ยนแปลง และปัญหาต่าง ๆ ภายในองค์การรวมทั้งปัจจัยเสริมทางสิ่งแวดล้อมอื่น ๆ ซึ่งไม่สามารถเปลี่ยนแปลงได้โดยบุคคลใดบุคคลหนึ่งหรือกลุ่มบุคคลใดกลุ่มบุคคลหนึ่ง แต่เป็นบุคคลทั้งองค์กร และมีการเปลี่ยนแปลงอย่างค่อยเป็นค่อยไป อย่างมีระเบียบแบบแผน

2.7.3.5 วัฒนธรรมองค์กรแห่งการตื่นรู้ (Awakening Culture)

ธรรมชาติขององค์กรมีลักษณะคล้ายกับธรรมชาติของชีวิตทั่วไป คือ เมื่อมีการกำเนิดขึ้น จะต้องมีการเติบโต มีการพัฒนา การพัฒนานั้นจะต้องเกิดขึ้นอย่างต่อเนื่องสม่ำเสมอ และมีการพัฒนาที่ยั่งยืนจึงจะทำให้องค์การอยู่รอดได้อย่างมั่นคง ซึ่งการอยู่รอดอย่างมั่นคงนั้นหมายถึง องค์กรต้องสามารถปรับตัวสอดรับกับกระแสการเปลี่ยนแปลงของสังคมและสิ่งแวดล้อมได้อย่างมีคุณภาพ มีลักษณะของการเรียนรู้อย่างไม่หยุดนิ่ง มีการตื่นตัวที่จะเรียนรู้อยู่ตลอดเวลา เพื่อให้เกิดการพัฒนาอย่างต่อเนื่อง ดังที่กล่าวมาแล้ว องค์กรที่มีลักษณะเช่นนี้ก็คือ องค์กรแห่งการตื่นรู้ “Awakening Organization” (เกศรา รักชาติ, 2549) ขณะเดียวกันองค์กรแห่งการตื่นรู้ก็มีลักษณะเป็น “องค์กรซึ่งสามารถปลดปล่อยศักยภาพของผู้ปฏิบัติงานออกมา ทำให้ผู้ปฏิบัติเกิดความมุ่งมั่นทุ่มเทเพื่อให้การทำงานขององค์กรบรรลุเป้าหมายที่วางไว้” ลักษณะขององค์กรแห่งการตื่นรู้จะมีลักษณะสำคัญที่ทำให้เกิดการเรียนรู้ที่โดดเด่น ดังที่เกศรา รักชาติ (2549) ได้สรุปไว้ดังนี้

1) ระดับความตื่นเต้น การตื่นตัว ความฮึกเหิม ความกระตือรือร้นของคนในองค์กรจะอยู่ในระดับสูง

2) ผู้คนในองค์กรส่วนใหญ่มีการตื่นตัว มีความเชื่อในสิ่งที่พวกเขาต้องการร่วมกัน มีการร่วมแรงร่วมใจกันสูง

3) ผู้คนในองค์กรมองเห็นความสำคัญของการเป็นส่วนหนึ่งขององค์กรมีความมุ่งมั่นในการทำงานร่วมกับผู้อื่นอย่างสร้างสรรค์ เห็นแก่ประโยชน์ส่วนรวมมากกว่าประโยชน์ส่วนตน

4) มีพื้นฐานการเรียนรู้ซึ่งกันและกัน ไว้เนื้อเชื่อใจกันสูง ทำให้มีการตัดสินใจที่รวดเร็ว มีการยอมรับและเคารพในการตัดสินของกันและกัน

5) คนในองค์กรมีความไว มีความยืดหยุ่น พร้อมที่ตอบสนองต่อสัญญาณแห่งการเปลี่ยนแปลงจากสภาพแวดล้อมทั้งภายในและภายนอก

6) มีวัฒนธรรมองค์กรแบบสร้างสรรค์ (Constructive Culture) ผู้นำในองค์กรทุกระดับมีความเชื่อในค่านิยมร่วม (Share Value) และแสดงออกทางพฤติกรรมถึงการปฏิบัติตามค่านิยมร่วมนั้น

7) บุคลากรในองค์กรมีการเจริญเติบโต มีความก้าวหน้า จะเห็นได้ว่าองค์กรแห่งการตื่นรู้นั้นจะมีพื้นฐานของการมีวัฒนธรรมแบบสร้างสรรค์ เน้นในเรื่องภาวะผู้นำทุกระดับจะสะท้อนให้เห็นผลงาน หรือ Performance ขององค์กรที่ชัดเจน ทำให้องค์กรมีการเจริญเติบโตอย่างต่อเนื่อง และมีพื้นฐานเป็นองค์กรแห่งการเรียนรู้ (Learning Organization) ที่แข็งแกร่งขึ้นนั่นเอง

การที่องค์กรจะเข้าสู่องค์กรแห่งการตื่นรู้ได้นั้น จำเป็นอย่างยิ่งที่ผู้บริหารองค์กร จะต้องมีความมุ่งมั่นและเห็นความสำคัญ ดังที่กล่าวมาแล้วโดยจะต้องกำหนดแนวทางการพัฒนาไปสู่เป้าหมายการเป็นองค์กรแห่งการตื่นรู้ ดังที่ สุรพงษ์ มาลี (2550) ได้เสนอแนวคิดการพัฒนาองค์กรแห่งการตื่นรู้ด้วยการปลุกจิตวิญญาณขององค์กร ปลุกภาวะผู้นำในตัวคน และปลุกคนอื่น ๆ ที่ทำงานร่วมกัน ดังนี้

1) ปลุกจิตวิญญาณองค์กร หมายถึง การทำให้พนักงานขององค์กรมีพลังเต็มเปี่ยม มีการกระตือรือร้น มีแรงบันดาลใจ มีความคิดสร้างสรรค์ ตลอดจนตระหนักรู้ในความหมายและความสำคัญของงานไม่ใช่ทำงานตามหน้าที่ไปวัน ๆ หนึ่ง ดังนั้นเมื่อจิตวิญญาณในองค์กรถูกปลุกผลงานขององค์กรก็จะได้รับการพัฒนาถึงขีดสุด สะท้อนออกมาในรูปแบบของผลผลิตที่มีคุณภาพมีความสร้างสรรค์

2) ปลุกภาวะผู้นำ หมายถึง การปลุกจิตวิญญาณของภาวะผู้นำให้ตื่นตัว โดยการปลุกภาวะผู้นำให้ตื่นตัวขึ้นมานั้น มีองค์ประกอบที่สำคัญ 10 ประการ คือ เป็นผู้มีความอ่อนน้อมถ่อมตน รู้จักตนเอง การทำในสิ่งที่ตนเองมีความสุข การเป็นผู้มีความฝันที่ยิ่งใหญ่ สภาพแห่งความสำเร็จในอนาคต หรือมีวิสัยทัศน์ มีความอดทน เป็นคนรักษาคำพูด เรียนรู้ประสบการณ์จากผู้ที่ประสบความสำเร็จ มีความเป็นตัวของตัวเอง และเป็นผู้นำที่เป็นผู้ให้ ซึ่งคุณลักษณะของการเป็นผู้นำทั้ง 10 ประการนี้ จะช่วยให้เกิดแรงบันดาลใจให้ผู้ตามเกิดความเชื่อมั่นในตัวผู้นำ ซึ่งจะนำพาให้องค์กรเกิดความก้าวหน้านั่นเอง

3) ปลุกคนรอบข้าง แม้ว่าผู้นำจะเป็นปัจจัยสำคัญที่จะนำพาองค์กรสู่องค์กรแห่งการตื่นรู้ แต่ผู้บริหารต้องมีการจูงใจและกระตุ้นเตือนให้คนอื่น ๆ ในองค์กรมีความมุ่งมั่นทุ่มเทและผูกพันกับองค์กร

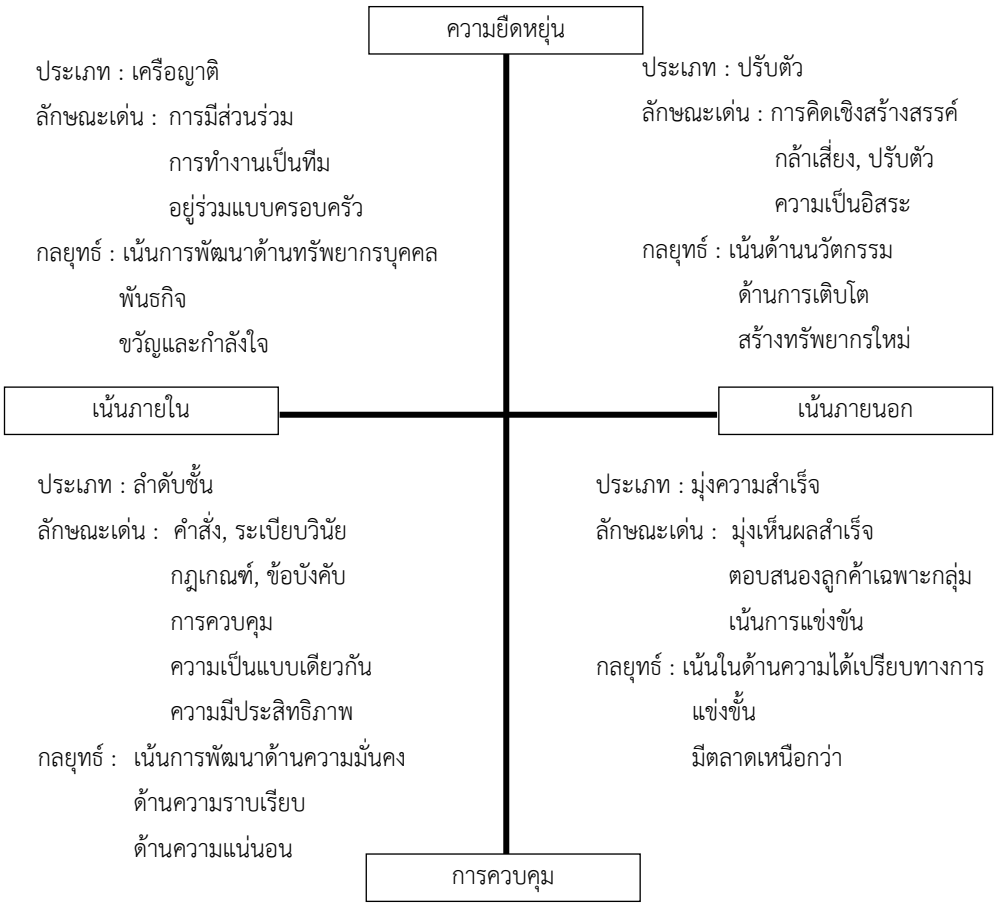
4) การสร้างและพัฒนาบุคลากรสำหรับองค์กรแห่งการตื่นรู้ การบริหารความรู้ และการให้ความสำคัญต่อกลุ่มคนที่ปฏิบัติงานบนฐานความรู้ มีความสำคัญอย่างยิ่งในการพัฒนาองค์กร ไปสู่การเป็นองค์กรแห่งการตื่นรู้ ต้องมีการปลุกหรือจูงใจผู้ปฏิบัติงาน เพื่อให้พวกเขาเปลี่ยนและนำความรู้ รวมทั้งประสบการณ์ที่สะสมในตัวออกมาใช้ให้เกิดประโยชน์เพื่อการบรรลุเป้าประสงค์ขององค์กร

ในปัจจุบันมีการแข่งขันระหว่างองค์กรสูง ทำให้มุมมองในการแบ่งประเภทของวัฒนธรรมองค์กรมุ่งเน้นไปที่คุณลักษณะที่เกี่ยวข้องกับการปฏิบัติงานขององค์กรโดยตรง ซึ่งรูปแบบที่พบได้บ่อยครั้งในการอ้างอิงการศึกษาด้านการบริหารจัดการ ได้แก่ รูปแบบของคาเมรอนและควิน, 2000 (Cameron and Quinn) ที่ทำการศึกษาและพัฒนาการแบ่งประเภทของวัฒนธรรมองค์กรเริ่มมา ตั้งแต่ปี 1980 จนถึงปัจจุบัน (วรวุฒิ กิจสิริวิศาล, 2553, หน้า 18-21) สำหรับการประเมินวัฒนธรรมองค์กรตามแนวคิดของ Cameron and Quinn. (2000) ใช้คุณลักษณะเฉพาะของวัฒนธรรมองค์กร 2 ด้าน ได้แก่ ประการแรก คือ ความยืดหยุ่น (Flexibility) กับเสถียรภาพ (Stability) และประการที่สอง คือ การเน้นปัจจัยภายนอก (External Focus) และการเน้นปัจจัยภายใน (Internal Focus) ซึ่งทำให้แบ่งวัฒนธรรมองค์ได้ 4 ประเภท ได้แก่ Clan Culture มีความยืดหยุ่นและการเน้นปัจจัยภายในสูง Adhocracy Culture มีความยืดหยุ่นและการเน้นปัจจัยภายนอก Market Culture มีเสถียรภาพและการเน้นปัจจัยภายนอก และ Hierarchy Culture มีเสถียรภาพและการเน้นปัจจัยภายใน เป็นต้น ส่วนประกอบของวัฒนธรรมองค์กรตามแนวคิดของ Cameron and Quinn. (2000) ประกอบด้วย 6 ประการ ได้แก่ ลักษณะเด่น (Dominant Characteristic) ความเป็นผู้นำ (Leadership) การจัดการคนในองค์กร (Management Employees) ความเป็นผู้นำ (Leadership) ความสัมพันธ์ในองค์กร (Organizational Glue) กลยุทธ์หลัก (Strategic Emphasis) และเงื่อนไขของความสำเร็จ (Criteria of Success) เป็นต้น

2.7.4 แบบประเมินวัฒนธรรมองค์กร (Organizational Culture Assessment Instrument : OCAI)

เครื่องมือประเมินวัฒนธรรมองค์กรถูกสร้างขึ้นมาจากนิยามร่วมสมัย (Contemporary) ของวัฒนธรรมองค์กรประกอบไปด้วย คุณค่า (Value) รูปแบบของผู้นำ (Leadership Style) กระบวนการทำงาน (Procedure) กิจวัตร (Routine) และมุมมองที่องค์กรมีต่อความสำเร็จ วัฒนธรรมองค์กรแสดงถึงคุณค่า สมมติฐาน ความคาดหวัง และเป็นสิ่งที่กำหนดลักษณะขององค์กร ในช่วงเวลานั้น ๆ (Cameron & Quinn 2000) ได้ทำการพัฒนาโครงร่าง (Framework) วัฒนธรรมองค์กรที่สร้างขึ้นบนทฤษฎีพื้นฐานเรียกว่า Competing Value Framework หรือแบบประเมินวัฒนธรรมองค์กร (Organizational Culture Assessment Instrument: OCAI) ซึ่งโครงร่างนี้จะสร้างให้เกิดแผนภูมิอันเกิดจากการอ้างอิง 2 ค่าของมิติหลักของวัฒนธรรมองค์กรในการ

วัดคุณลักษณะ 6 ประการของวัฒนธรรมองค์กร ดังที่กล่าวไปแล้วข้างต้น โดยมิติแรก คือ การเปรียบเทียบระหว่างลักษณะเด่นขององค์กรในด้านความยืดหยุ่น (Flexibility) ความเป็นอิสระ (Individual) และความเข้มงวด (Stability) การควบคุม (Control) ซึ่งบ่งชี้ว่าองค์กรมีลักษณะเหมือนสิ่งมีชีวิต (Organic) หรือเครื่องจักร (Mechanistic) ในส่วนของมิติที่ 2 ได้แก่ การให้ความสำคัญภายใน (Internal) หรือภายนอก (External) ขององค์กร เพื่อสร้างให้เกิดรูปร่างองค์กรในลักษณะของแผนภูมิเรดาร์ (Radar Chart) ซึ่งจะสามารถแบ่งประเภทของวัฒนธรรมองค์กรจากแบบประเมิน 4 ประเภท มีรายละเอียดดังนี้ (วรวุฒิ กิจสิริวิศาล, 2553, หน้า 31-35) ดังภาพประกอบที่ 2.3



ภาพประกอบที่ 2.3 แบบจำลองประเภทวัฒนธรรมองค์กร

1) วัฒนธรรมแบบเครือญาติ (Clan Culture) มีความยืดหยุ่นและการเน้นปัจจัยภายในสูง ลักษณะขององค์กรมีลักษณะคล้ายกับครอบครัวขยายเต็มไปด้วยการมีส่วนร่วมในการกำหนดคุณค่าและเป้าหมายขององค์กร การผูกพัน (Commitment) ของคนในองค์กรต่อองค์กรอยู่

ในระดับที่ดี เทียบเท่ากับที่องค์กรให้ ความสำเร็จของงานเกิดขึ้นโดยทีมงานที่สามารถทำการตัดสินใจได้ด้วยตัวเอง และมีลูกค้าที่มีลักษณะเหมือนกับเป็นผู้ร่วมงาน (Partner)

2) วัฒนธรรมแบบปรับตัว (Adhocracy Culture) มีความยืดหยุ่นและการเน้นปัจจัยภายนอกสูง เป็นลักษณะขององค์กรที่ก่อตั้งใหม่หรือองค์กรเฉพาะกิจโดยทั่วไป สภาพแวดล้อมส่งผลให้องค์กรมีการปฏิบัติงานที่มีความยืดหยุ่นสูง สำหรับคนในองค์กรมีแรงกระตุ้นจากนวัตกรรม (Innovative) ความสร้างสรรค์ (Creative) และลักษณะการลงทุน มีการกระจายอำนาจสู่ทีมงานและตัวบุคคล ปัจจัยภายนอกเป็นตัวแปรสำคัญในการสร้างวัฒนธรรมองค์กรประเภทนี้ รวมทั้งเกิดจากการที่ผู้นำเชิงกลยุทธ์มุ่งสร้างค่านิยมใหม่ขององค์กรที่เอื้อต่อการเพิ่มขีดความสามารถในการตีความหรือคาดการณ์ภาวะแวดล้อมภายนอก เพื่อให้เกิดพฤติกรรมในองค์กรที่สามารถตอบสนองได้ตลอดเวลา พนักงานขององค์กรจึงได้รับความอิสระในการตัดสินใจเองและพร้อมลงมือปฏิบัติได้ทันทีเมื่อเกิดความจำเป็น โดยยึดค่านิยมในการตอบสนองต่อลูกค้าเป็นสำคัญ ผู้นำมีบทบาทสำคัญต่อการสร้างความ เปลี่ยนแปลงให้เกิดขึ้นกับองค์กรด้วยการกระตุ้นพนักงานให้กล้าเสี่ยง กล้าทดลองคิดทำในสิ่งใหม่ และเน้นการให้รางวัลผลตอบแทนแก่ผู้ที่ริเริ่มสร้างสรรค์เป็นพิเศษ

3) วัฒนธรรมแบบมุ่งความสำเร็จ (Market Culture) มีเสถียรภาพและการเน้นปัจจัยภายนอกสูง เป็นองค์กรที่ถูกกำหนดด้วยปัจจัยภายนอกแต่มีการวางอำนาจภายในแบบรวมศูนย์ ซึ่งเป็นลักษณะเฉพาะที่ทำให้แตกต่างจาก Adhocracy Culture ประสิทธิผลขององค์กรวัดที่ความสามารถในการทำกำไร และส่วนแบ่งทางการตลาด คุณค่าหลักขององค์กร คือ ความสามารถในการแข่งขันและความสามารถในการผลิตที่มีการวัดผลในองค์กรเทียบกับอดีตและการคาดการณ์ในอนาคต รวมทั้งการมีวิสัยทัศน์ที่ชัดเจนของเป้าหมายองค์กร ผู้นำมุ่งเห็นผลสำเร็จของเป้าหมาย เช่น ตัวเลขยอดขายเพิ่ม ผลประกอบการมีกำไร เป็นต้น องค์กรมุ่งให้บริการลูกค้าพิเศษเฉพาะกลุ่มในภาวะแวดล้อมภายนอก แต่ไม่เห็นความจำเป็นที่จะต้องมีความยืดหยุ่นและต้องเปลี่ยนแปลงรวดเร็วแต่อย่างใด องค์การที่ยึดวัฒนธรรมแบบมุ่งความสำเร็จจึงเน้นค่านิยมแบบแข่งขันเชิงรุก

4) วัฒนธรรมแบบลำดับชั้น (Hierarchy Culture) มีเสถียรภาพและการเน้นปัจจัยภายในสูง เป็นรูปแบบขององค์กรราชการ องค์กรสาธารณะทั่วไป หรือองค์กรที่มีอายุเก่าแก่เพราะองค์กรดังที่กล่าวมาเป็นองค์กรที่มีรูปแบบของการทำงานที่คงที่ สม่ำเสมอ เป็นองค์กรที่ต้องมีความ น่าเชื่อถือ มีกฎระเบียบในการปกครองและมีกระบวนการทำงานที่เป็นมาตรฐานกับทุกคนในองค์กร อย่างไรก็ตามในปัจจุบันที่สภาพแวดล้อมมีการเปลี่ยนแปลงทำให้องค์กรประเภทนี้มีการเปลี่ยนแปลง องค์ประกอบบางอย่างในองค์กร และให้ความสำคัญต่อภาวะแวดล้อมภายในความคงเส้นคงวาในการ ดำเนินการเพื่อให้เกิดความมั่นคง โดยมุ่งเน้นด้านวิธีการ ความเป็นเหตุผลความมีระเบียบในการทำงาน มุ่งเน้นเรื่องให้ยึดและปฏิบัติตามกฎระเบียบ ยึดหลักการประหยัดความสำเร็จขององค์กรเกิดจากความสามารถในการบูรณาการและความมีประสิทธิภาพ

2.8 แนวคิดเกี่ยวกับความรู้ (Knowledge)

การแบ่งประเภทของความรู้ มองได้หลายมิติ แต่มิติที่ได้รับความนิยมมากที่สุด คือ มองในด้าน “รูปแบบที่มองเห็น” ซึ่ง ชู (Choo,2000 : 26 – 28) ได้แบ่งความรู้เป็น 3 ประเภท คือ

2.8.1 ความรู้โดยนัย (Tacit หรือ Implicit Knowledge) หมายความถึงเป็นความรู้เฉพาะตัวที่เกิดจากประสบการณ์ การศึกษา การสนทนา การฝึกอบรม ความเชื่อ เจตคติของแต่ละบุคคล เป็นความรู้บวกกับสติปัญญา และประสบการณ์ ซึ่งถือได้วาเป็นองค์รวมของความรู้ของแต่ละบุคคล ซึ่งเป็นความรู้ที่ไม่อยู่นิ่ง จะปรับเปลี่ยนไปตามสถานการณ์ของการใช้ความรู้ของแต่ละคน ซึ่งก็คือความรู้ที่ผ่านกระบวนการขัดเกลาทางสังคม ซึ่งถือว่าเมื่อคนปฏิบัติงานนาน ๆจนเกิดความช่ำชอง ความรู้ประเภทนี้ถือเป็นความรู้ไม่เป็นทางการจัดระบบหรือจัดหมวดหมู่ไม่ได้ แต่สามารถแลกเปลี่ยนหรือนำมาเล่าสู่กันฟง สามารถถ่ายทอดแบ่งปันความรู้นี้ได้และสามารถสังเกตและเลียนแบบได้ ซึ่งองค์การต้องตองพยายามปรับเปลี่ยนความรู้โดยนัย ให้เป็นความรู้ที่ปรากฏเพื่อเป็นความรู้ที่ฝังกับองค์การ (Embedded Knowledge) ไม่ยึดติดกับตัวบุคคล

2.8.3 ความรู้ที่ปรากฏ (Explicit Knowledge) เป็นความรู้ที่ได้รับการถ่ายทอดจากบุคคลออกมาในรูปของบันทึกในรูปแบบต่าง ๆ ซึ่งก็คือ สารสนเทศนั่นเอง เช่น หนังสือ บทความ เอกสาร มาตรฐาน ลิขสิทธิ์ สิทธิบัตร เครื่องหมายการค้า ความลับทางการค้า รายงานประจำปี สื่อโสตทัศน์ เช่น วีดีโอ ซีดี สื่ออิเล็กทรอนิกส์ เช่น ไปรษณีย์อิเล็กทรอนิกส์ อินเทอร์เน็ต เว็บไซต์ อี-บุค ความรู้ที่ปรากฏถือได้ว่ามีการใช้สัญลักษณ์ ไม่ว่าจะเป็นภาษาพูด ภาษาเขียนเพื่อบันทึกความรู้นั้น ๆ ทำให้คนเข้าใจได้กว้างขวาง และสะดวกยิ่งขึ้นความรู้ที่มีการสะสมกันมานานเป็นความรู้ที่ใช้ประโยชน์ได้อย่างมีประสิทธิภาพและมีการตรวจสอบอย่างเป็นระบบ

2.8.3 ความรู้ที่เกิดจากวัฒนธรรม (Culture Knowledge)

เป็นความรู้ที่เกิดจากความเชื่อศรัทธา ซึ่งจะเกิดจากผลสะท้อนกลับของตัวความรู้และสภาพแวดล้อมขององค์การ องค์การที่พัฒนามาเป็นระยะเวลานานจะมีการพัฒนาความเชื่อร่วมกันในเรื่องที่เกี่ยวกับธรรมชาติขององค์การ ความสามารถหลักขององค์การ (Core Competency) ซึ่งก็คือวัฒนธรรมขององค์การนั่นเอง

Good (1973, p. 325) กล่าวว่า ความรู้เป็นข้อเท็จจริง (Fact) ความจริง (Truth) เป็นข้อมูลที่มนุษย์ได้รับและเก็บรวบรวมจากประสบการณ์ต่าง ๆ การที่บุคคลยอมรับหรือปฏิเสธสิ่งใดสิ่งหนึ่งได้อย่างมีเหตุผล บุคคลควรจะต้องรู้เรื่องเกี่ยวกับสิ่งนั้น เพื่อประกอบการตัดสินใจ นั่นคือบุคคลจะมีข้อเท็จจริงหรือข้อมูลต่าง ๆ ที่สนับสนุนและให้คำตอบข้อสงสัยที่มีอยู่สามารถชี้แจงให้เกิดความเข้าใจและมีทัศนคติอันดี ตลอดจนเกิดความตระหนัก ความเชื่อ และค่านิยมต่าง ๆ ด้วย

เบอร์กูน (Burgoon, 1974, p. 64) กล่าวว่า การที่ผู้รับสารมีระดับการศึกษา หรือเคยศึกษาในสาขาวิชาที่ต่างกัน ตลอดจนได้รับการศึกษาในยุคสมัยที่แตกต่างกัน จะส่งผลให้มีความรู้

ความนึกคิด และอุดมการณ์ที่แตกต่างกัน โดยชวงเวลาของการเปิดรับสารมีอิทธิพลต่อความรู้ของผู้รับสาร

สุชาติ วงษ์หุน (2539, น.28) กล่าวว่า ความรู้เป็นพฤติกรรมเบื้องตนที่ผู้เรียนสามารถจดจำได้หรือระลึกได้ โดยการมองเห็นหรือได้ยิน ซึ่งความรู้ในที่นี้คือขอเท็จจริง กฎเกณฑ์คำจำกัดความ เป็นต้น โดยขั้นนี้ความรู้จึงเป็นพฤติกรรมขั้นต้นที่คนเราเพียงแต่จำได้ อาจจะโดยการนึกได้ ความรู้ขั้นนี้ได้แก่ ความรู้ที่เกี่ยวกับคำจำกัดความ ความหมาย ข้อเท็จจริง ทฤษฎี กฎโครงสร้าง และวิธีการแก้ปัญหา ดังนั้น อาจกล่าวรวม ๆ ได้ว่า ความรู้ หมายถึง การเรียนรู้ที่เน้นความจำ และการระลึกถึงได้ของคนเราที่มีต่อความคิด ปรากฏการณ์ หรือวัตถุต่าง ๆ ความจำนี้อาจเริ่มจากสิ่งที่ง่ายไม่ซับซ้อนไปจนถึงเรื่องยุ่งยากซับซ้อนขั้นได้

ความรู้ เป็นการรับรู้เบื้องต้น ซึ่งบุคคลส่วนมากจะได้รับผ่านประสบการณ์ โดยการเรียนรู้จากการตอบสนองต่อสิ่งเร้า (Stimulus-Response) แล้วจัดระบบเป็นโครงสร้างของความรู้ที่ผสมผสานระหว่างความจำ (ข้อมูล) กับสภาพจิตวิทยา ดังนั้น ความรู้ จึงเป็นความจำที่เลือกสรรให้สอดคล้องกับสภาพจิตใจของตนเอง ความรู้จึงเป็นกระบวนการภายใน อย่างไรก็ตามความรู้ก็อาจส่งผลต่อพฤติกรรมที่แสดงออกของมนุษย์ อาจปรากฏได้จากจากสาเหตุ 5 ประการ คือ (สุรพงษ์ โสธนะ เสถียร, 2533, น. 120-121)

1. การตอบข้อสงสัย (Ambiguity Resolution) การสื่อสารมักสร้างความสับสนให้สมาชิกในสังคม ผู้รับสารจึงมักแสวงหาสารสนเทศโดยอาศัยสื่อทั้งหลาย เพื่อตอบข้อสงสัยและความสับสนของตน

2. การสร้างทัศนะ (Attitude Formation) ผลกระทบเชิงความรู้ต่อการปลูกฝังทัศนะนั้น ส่วนมากนิยมใช้กับสารสนเทศที่เป็นนวัตกรรม เพื่อสร้างทัศนคติให้คนยอมรับการแพร่นวัตกรรมนั้น ๆ (ในฐานะความรู้)

3. การกำหนดวาระ (Agenda Setting) เป็นผลกระทบเชิงความรู้ที่สื่อกระจายออกไปเพื่อให้ประชาชนตระหนักและผูกพันกับประเด็นวาระที่สื่อกำหนดขึ้น หากตรงกับภูมิหลังของปัจเจกชนและค่านิยมของสังคมแล้ว ผู้รับสารก็จะเลือกสารสนเทศนั้น

4. การพอกพูนระบบความเชื่อ (Expansion of The Belief System) การสื่อสารสังคม มักกระจายความเชื่อ ค่านิยม และอุดมการณ์ด้านต่าง ๆ ไปสู่ประชาชน จึงทำให้ผู้รับสารรับทราบระบบความเชื่อถือหลากหลาย และลึกซึ้งไว้ในความเชื่อของตนมากขึ้นเรื่อย ๆ

5. การรู้แจ้งต่อค่านิยม (Value Clarification) ความขัดแย้งในเรื่องค่านิยมและอุดมการณ์เป็นภาวะปกติของสังคม สื่อมวลชนที่นำเสนอข้อเท็จจริงในประเด็นเหลานี้ ย่อมทำให้ประชาชนผู้รับสารเข้าใจถึงค่านิยมเหลานั้นแจ้งชัดขึ้น

บลูม และคณะ (Bloom et al., 1956, p. 28, อ้างถึงใน อรวรรณ ปลันธนโอวาท, 2549, น. 36-37) ได้แยกการประเมินระดับความรู้ไว้ 6 ระดับ ดังนี้

1. ระดับที่ระลึกได้ (Recall) หมายถึง การเรียนรู้ในลักษณะที่จำเรื่องเฉพาะ วิธีปฏิบัติกระบวนการ และแบบแผนได้ ความสำเร็จในระดับนี้ คือ ความสามารถในการดึงข้อมูลจากความจำออกมาได้

2. ระดับที่รวบรวมสาระสำคัญได้ (Comprehension) หมายถึง บุคคลสามารถทำบางสิ่งบางอย่างได้มากกวาการจำเนื้อหาที่ได้รับ สามารถเขียนข้อความนั้นได้ ด้วยถ้อยคำของตนเอง สามารถแสดงให้เห็นได้ด้วยภาพ ให้ความหมาย แปลความหมาย และเปรียบเทียบความคิดอื่น ๆ หรือคาดคะเนผลที่เกิดขึ้นต่อไปได้

3. ระดับของการนำไปใช้ (Application) สามารถนำเอาข้อเท็จจริงและความคิดเห็นที่เป็นนามธรรม (Abstract) ไปปฏิบัติการจริงอย่างเป็นรูปธรรม

4. ระดับของการวิเคราะห์ (Analysis) สามารถให้ความคิดเห็นในรูปของการนำความคิดมาแยกเป็นสวน เป็นประเภท หรือการนำข้อมูลมาประกอบกันเพื่อการปฏิบัติของตนเอง

5. ระดับของการสังเคราะห์ (Synthesis) คือ การนำเอาข้อมูล แนวความคิดนำมาประกอบกัน แล้วนำไปสู่การสร้างสรรค์ (Creative) สิ่งใหม่ที่แตกต่างไปจากเดิม

6. ระดับของการประเมินผล (Evaluation) คือ ความสามารถในการใช้ข้อมูลเพื่อตั้งเกณฑ์ (Criteria) การรวบรวมผล และวัดข้อมูลตามมาตรฐาน เพื่อให้ตั้งข้อตัดสินถึงระดับของประสิทธิผลของกิจกรรมแต่ละอย่าง

2.9 แนวคิดเกี่ยวกับความตระหนักรู้

พจนานุกรมราชบัณฑิตสถาน พ.ศ. 2542 (2546) ได้ให้ความหมาย “ความตระหนักว่าเป็นการรู้ประจักษ์ชัด รู้ชัดแจ้ง” โดยสอดคลองกับพจนานุกรม ของ Good (1973, p. 54) โดยได้ให้ความหมายว่า “การแสดงออกจากการระลึกได้หรือจดจำได้” นอกจากนั้น ยังมีผู้นิยามไว้อีก ดังนี้

Bloom (1971, p. 271 อ้างถึงใน สุพัตรา ถนอมวงค์, 2551, น.10) ได้ให้นิยามว่า “ความตระหนัก คือ ภาคต่ำสุดทางภาคอารมณ์ซึ่งความตระหนักนั้นคล้ายกับอารมณ์ความรู้สึก (Affective Domain) แต่ความตระหนักต่างกับความรู้สึกตรงที่ความตระหนักไม่จำเป็นต้องเน้นปรากฏการณ์หรือสิ่งหนึ่งสิ่งใด แต่ความตระหนักจะเกิดขึ้นเมื่อมีสิ่งเราให้เกิดความตระหนัก”

กุลวดี ราชภักดี (2545, น.38) ได้ให้นิยามว่า “ความตระหนัก หมายถึง การที่บุคคลเกิดความรู้สึก นึกคิด ความคิดเห็นหรือประสบการณ์แล้วเกิดความเข้าใจแล้วประเมินสถานการณ์ที่เกี่ยวกับตนเองได้จากสภาวะจิตที่ยอมรับและเกิดแสดงพฤติกรรมตอบสนองต่อเหตุการณ์”

อนุสรณ กาลดิษฐ (2548, น.51) ได้ให้นิยามว่า “ความตระหนัก หมายถึง ความสำนึกของแต่ละบุคคลเคยมีการรับรู้หรือเคยมีความรู้มาก่อน มีสิ่งเร้ามากระตุ้นจนเกิดความตระหนักจากการประเมินค่า”

ประพล มิลินทจินดา (2542, น.19) ได้ให้นิยามว่า “ความตระหนัก คือ การแสดงความรู้สึกนึกคิด ความคิดเห็น ที่บุคคลเข้าใจและประเมินสถานการณ์ที่เกิดขึ้นเกี่ยวกับตนเองจากประสบการณ์จากช่วงระยะเวลา จากเหตุการณ์ และจากสภาพแวดล้อม เป็นปัจจัยทำให้มนุษย์มีความตระหนัก”

วีระชน ขาวผ่อง (2551,น.42) ได้ให้นิยามว่า “ความตระหนัก คือ สภาวการณ์มีผลให้เกิดความรู้สึก การรับรู้มุ่งสู่สภาวะจิตแห่งตน คือ ทัศนคติ ความคิด ความเชื่อ ความสนใจ อันจะก่อให้เกิดความตระหนักและจิตสำนึก”

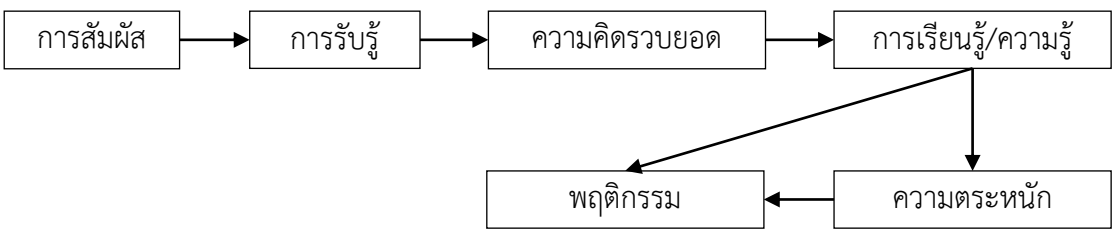
พงษชัย เฉลิมกลิ่น (2551,น. 50) ได้ให้นิยามว่า “ความตระหนัก คือ พฤติกรรมที่แสดงถึงความรับผิดชอบต่อสิ่งใดสิ่งหนึ่งหรือเหตุการณ์ใดเหตุการณ์หนึ่ง ซึ่งเป็นอารมณ์ความรู้สึกด้านทัศนคติ ค่านิยม ความชอบหรือไม่ชอบ ดีหรือไม่ดี ที่ได้จากการประเมินสิ่งเร้าต่าง ๆ ของบุคคลนั้น”

ทั้งนี้สามารถสรุปได้ว่า ความตระหนัก (Awareness) คือ การรับรู้แบบฉุกคิดขึ้นมากะทันหันต่อสิ่งใดสิ่งหนึ่งหรือเหตุการณ์ใดเหตุการณ์หนึ่งซึ่งเป็นอารมณ์ความรู้สึกโดยอาศัยองค์ประกอบจากสิ่งแวดล้อม ประสบการณ์ และสิ่งที่ส่งผลกับอารมณ์และความรู้สึก

2.9.1 ปัจจัยที่ทำให้เกิดความตระหนัก

กระบวนการเกิดความตระหนักมาจากกระบวนการทางปัญญา (Cognitive process) ทั้งนี้ เมื่อบุคคลได้รับการกระตุ้นจากสิ่งเร้าหรือรับสัมผัสจากสิ่งเร้าหรือประสบการณ์แล้วจะเกิดการรับรู้ จากนั้นจะเข้าใจในสิ่งเร้านั้น และเกิดเป็นความคิดรวบยอด และทำให้มีความรู้ (Knowledge) และเมื่อมีความรู้ในสิ่งนั้นก็จะนำไปสู่การเกิดความตระหนัก ทั้งนี้ความรู้และความตระหนักนี้ต่างก็จะนำไปสู่การกระทำ (Action) หรือการแสดงพฤติกรรมของบุคคลต่อสิ่งเร้านั้น ๆ

พจนานุกรม ของ Good (1973) ได้ประมวลขั้นตอนของกระบวนการเกิดความตระหนักดังนี้ (Good, 1973 อ้างถึงใน สุธาสินีอินทร์ผูก, 2548) ดังภาพประกอบที่ 2.4



ภาพประกอบที่ 2.4 ขั้นตอนของกระบวนการเกิดความตระหนัก

ในลักษณะเช่นนี้ความตระหนักจึงเป็นผลของกระบวนการทางปัญญา กล่าวคือ เมื่อบุคคลได้รับการกระตุ้นจากสิ่งเร้า หรือรับสัมผัสจากสิ่งเร้าแล้วเกิดการรับรู้ขึ้นแล้วจะนำไปสู่การเกิด

ความเข้าใจในสิ่งเร้านั้น และนำไปสู่การเรียนรู้เป็นขั้นตอนต่อไป และเมื่อบุคคลเกิดมีความรู้ในสิ่งนั้นแล้วก็จะมีผลไปสู่ความตระหนักในที่สุด ซึ่งทั้งความรู้และความตระหนักจะนำไปสู่การกระทำหรือพฤติกรรมของบุคคลที่มีต่อสิ่งเร้านั้น ๆ ต่อไป และจากการศึกษาของทนงศักดิ์ ประสบกิตติคุณ (ม.ป.ป. อ้างถึงใน พัฒนศักดิ์บุบผาสุวรรณ, 2546) กล่าวถึง ปัจจัยทางพฤติกรรมศาสตร์ที่มีผลต่อความตระหนัก ประกอบด้วย ประสบการณ์ที่มีต่อการรับรู้ความเคยชินต่อสภาพแวดล้อม ถ้าบุคคลใดไม่เคยชินต่อสภาพแวดล้อมนั้นก็จะทำให้บุคคลนั้นไม่ตระหนักต่อสิ่งที่เกิดขึ้น ความใส่ใจและการให้คุณค่า ถ้ามนุษย์มีความใส่ใจในเรื่องใดมากก็จะมี ความตระหนักในเรื่องนั้นมาก ลักษณะและรูปแบบของสิ่งเร้า ถ้าสิ่งเร้านั้นสามารถทำให้ผู้พบเห็นเกิดความสนใจย่อมทำให้ผู้พบเห็นเกิดการรับรู้และความตระหนักขึ้น ระยะเวลาและความถี่ในการรับรู้ ถ้ามนุษย์ได้รับรู้บ่อยครั้งเท่าใดก็ยิ่งทำให้มีโอกาสเกิดความตระหนักได้มากขึ้นเท่านั้น

สำหรับวิธีการสร้างความตระหนักทำได้ด้วยวิธีดังต่อไปนี้

1) การเผยแพร่ข้อมูล

2) สร้างข้อความที่มีผลกระทบสูง หรือข้อความที่กระตุ้นอารมณ์

3) สร้างข้อความที่เชื่อมต่อทัศนคติกับพฤติกรรมที่ผ่านมา

อย่างไรก็ตาม ลักษณะเฉพาะของแต่ละบุคคลมีผลต่อการรับรู้และการเกิดความตระหนักที่มุ่งเน้นการเปลี่ยนแปลงการรับรู้เกี่ยวกับกลุ่มหรือต่อวัตถุ รวมทั้งจะเกิดความตระหนักต่อสถานการณ์ที่จะส่งเสริมการเปลี่ยนแปลงทัศนคติต่างกัน

นอกจากนี้ Herek, G. (1986,pp99 -104) กล่าวว่า ปัจจัยด้านสถานการณ์ที่ทำให้บุคคลมีความตระหนักมากขึ้นสวนหนึ่งมาจากการรับรู้ข่าวสาร อย่างไรก็ตามยังไม่อาจสามารถสรุปได้ว่าทัศนคติและความตระหนักมีผลโดยตรงทำให้เกิดการเปลี่ยนแปลงพฤติกรรม แต่เป็นเพียงปัจจัยที่มีส่วนให้เกิดการเปลี่ยนแปลงพฤติกรรมเท่านั้น เช่นเดียวกันกับ Kim, M. s., & Hunter, J. e. (1993, pp. 331 - 364) อธิบายว่า ความตระหนักรู้ทำหน้าที่เป็นตัวกลางในการมีปฏิสัมพันธ์เชิงทัศนคติและพฤติกรรมความตระหนักรู้สร้างความเต็มใจในการมีส่วนร่วมกับพฤติกรรมต่าง ๆ

2.10 งานวิจัยที่เกี่ยวข้อง

กริน ธัญญวิกรม และ ธีระ กุลสวัสดิ์ (2564) บทความวิจัยเรื่อง การจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ กรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย ผู้วิจัยเห็นว่าควรมีข้อเสนอแนะที่เป็นนัยยะในเชิงนโยบายที่สำคัญ ดังนี้

1) รัฐควรเร่งรัดการบังคับใช้ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์และ พ.ร.บ.การคุ้มครองข้อมูลส่วนบุคคล โดยการออกกฎหมายลูกและประกาศกฎเกณฑ์ต่าง ๆ เพื่อให้การดำเนินการมีความสอดคล้องและเป็นไปในทิศทางเดียว

2) ธนาคารควรส่งเสริมให้ความรู้และตะหนักถึงภัยคุกคามไซเบอร์ และภัยคุกคามทางการเงินในการทำธุรกรรมการเงินทางอิเล็กทรอนิกส์ให้กับประชาชนและลูกค้าของธนาคารให้มากขึ้น

3) ภาคประชาชนควรจะเรียนรู้และตะหนักถึงภัยคุกคามไซเบอร์ ภัยคุกคามทางการเงินในการทำธุรกรรมการเงินทางอิเล็กทรอนิกส์

นาวาอากาศเอก ชนินทร เฉลิมทรัพย์ (2561) การวิจัยเรื่อง แนวทางการบูรณาการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ ผู้วิจัยได้ศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กร การบูรณาการการบริหารจัดการและการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งศึกษาค้นคว้านโยบายยุทธศาสตร์และการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงกลาโหมและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จากการวิจัยนี้ได้มีข้อเสนอแนะว่าสำหรับแนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ คือ

1) การจัดการความรู้และการบริหารความเสี่ยง (Knowledge Management & Risk) เพื่อให้ผู้นำองค์กร ผู้กำหนดนโยบายและผู้ปฏิบัติ ได้ตระหนักรู้ เก็บสะสมองค์ความรู้ และประสบการณ์เพื่อเป็นประโยชน์ต่อไป

2) มีการทำงานแบบเครือข่ายเชื่อมโยงตามประเด็นยุทธศาสตร์ร่วม (Common Agenda) ปฏิบัติงานตามมาตรฐานการปฏิบัติทางเทคโนโลยีและจัดตั้งศูนย์การศึกษาการวิจัยการพัฒนาด้านความมั่นคงปลอดภัยทางไซเบอร์ต่อไป

นายสุธาเทพ รุณเรศ (2561) วิจัยเรื่อง ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร การวิจัยดังกล่าวผู้วิจัยได้มีการวิจัยเชิงสำรวจประชากรกับผู้ใช้อินเตอร์เน็ตที่มีอายุ 15 ปีขึ้นไปและอยู่ในเขตกรุงเทพมหานคร พบว่า ปัจจัยที่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเตอร์เน็ต ประกอบด้วย ปัจจัยทางด้านลักษณะทางประชากรด้านอายุ ระดับการศึกษา รายได้ส่วนตัวต่อเดือน และด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ แต่ปัจจัยทางด้านประสบการณ์เกี่ยวกับคุกคามทางไซเบอร์และปัจจัยทางด้านลักษณะทางประชากรทางเพศไม่มีผลต่อความตระหนักถึงภัยคุกคามไซเบอร์ของผู้ใช้งานอินเตอร์เน็ต

ผู้วิจัยได้ให้ข้อเสนอแนะว่าหากจะทำการวิจัยเกี่ยวกับภัยคุกคามทางไซเบอร์ ดังนี้ ควรมีการศึกษาปัจจัยทางสังคมที่อาจมีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเตอร์เน็ต ควรจะใช้การวิจัยเชิงคุณภาพด้วยการสัมภาษณ์กลุ่มหรือการสัมภาษณ์เจาะลึกเพื่อศึกษาความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในเชิงลึกและข้อมูลที่รอบด้านครบมิติมากยิ่งขึ้น รวมทั้งควรมีการศึกษานโยบายของรัฐและองค์กรต่างๆเกี่ยวกับการป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต

สุรพงษ์ ทรัพยากร และ อรรถพล ป้อมสถิตย์ (2563) การวิจัยเรื่อง การวิเคราะห์การรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

พ.ศ. 2562 จากการวิจัยพบว่าธนาคารพาณิชย์นี้จะต้องมีการปรับปรุงพัฒนาเพื่อสร้างความเข้มแข็งในด้านเทคโนโลยีสารสนเทศทั้ง 3 ด้าน คือ

1) การใช้เทคโนโลยีที่เหมาะสมสำหรับบูรณาการในด้านเทคนิค

2) มีการสร้างแบบนโยบายหรือแนวทางปฏิบัติสำหรับกำกับผู้ปฏิบัติงานเพื่อลด ความเสี่ยงหรือภัยคุกคามที่มาจากความผิดพลาดของมนุษย์

3) มีการเตรียมความพร้อมหรือมีมาตรการรองรับสำหรับด้านภัยหรือสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้น

Kabanda, Gabriel. (2018). การวิจัยหัวข้อ A Cybersecurity Culture Framework and Its Impact on Zimbabwean Organizations มีวัตถุประสงค์เพื่อพัฒนากรอบวัฒนธรรมความปลอดภัยทางไซเบอร์และประเมินผลกระทบต่อองค์กร กล่าวคือ “จะพัฒนากรอบวัฒนธรรมความปลอดภัยในโลกไซเบอร์เพื่อแก้ปัญหาความปลอดภัยทางไซเบอร์สำหรับผู้ใช้ระดับรากหญ้าของไซเบอร์สเปซในซิมบับเวได้อย่างไร?”

วัฒนธรรมความปลอดภัยทางไซเบอร์ กล่าวถึง ประเด็นทางเศรษฐกิจ กฎหมาย และสังคมที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ เพื่อช่วยให้สังคมได้พร้อมเผชิญความท้าทายที่เกี่ยวข้องกับการใช้และการนำเทคโนโลยีไปใช้ในทางที่ผิด กรอบงาน NIST Cybersecurity เป็นกรอบความมั่นคงปลอดภัยทางไซเบอร์ที่จะสนับสนุนวัฒนธรรมความปลอดภัยทางไซเบอร์เพื่อป้องกันการโจมตีทางไซเบอร์ ที่เปลี่ยนแปลงความคิดของผู้คนและพฤติกรรมของพวกเขา และจะเป็นไฟร์วอลล์ของมนุษย์ที่แข็งแกรงในการต่อต้านภัยคุกคามโดยไม่มีการบังคับ และเป็นสิ่งจำเป็นตามที่สถาบันมาตรฐานและเทคโนโลยีแห่งชาติสร้างขึ้น โดยคำนึงถึงการลดความเสี่ยงทางไซเบอร์และปรับปรุงการรักษาความปลอดภัยให้กับโครงสร้างพื้นฐานที่สำคัญ

Uchendu Betsy, Nurse R.C., Bada Maria & Furnell Steven. (2021). เรื่อง Developing a cyber security culture: Current practices and future needs. ศึกษาวิจัยเกี่ยวกับวัฒนธรรมความปลอดภัยทางไซเบอร์ขององค์กร การกำหนดวัฒนธรรมความปลอดภัยในโลกไซเบอร์ ปัจจัยใดที่จำเป็นต่อการสร้างและรักษาวัฒนธรรม กรอบงานที่เสนอเพื่อปลูกฝังวัฒนธรรมความปลอดภัย และตัวชี้วัดที่แนะนำให้ประเมินด้วยการใช้เทคนิคการทบทวนวรรณกรรมอย่างเป็นระบบของ PRISMA โดยการวิเคราะห์บทความวิจัย 58 บทความจากช่วง 10 ปีที่ผ่านมา (2010-2020) ผลการวิจัยแสดงให้เห็นว่า แม้ว่าบทความเหล่านั้นจะมีการใช้คำต่างๆ เช่น วัฒนธรรมการรักษาความปลอดภัยข้อมูลและวัฒนธรรมการรักษาความปลอดภัยทางไซเบอร์ ผลการวิจัยจากบทความเหล่านั้นได้ข้อสรุปมีความคล้ายคลึงกันว่า

1. ปัจจัยที่มีอิทธิพลมากที่สุด ได้แก่ การสนับสนุนผู้บริหารระดับสูง นโยบายและขั้นตอน และการรับรู้มีความสำคัญอย่างยิ่งในการสร้างวัฒนธรรมความปลอดภัยในโลกไซเบอร์

2. กรอบงานจำนวนมากที่ตรวจสอบแล้วพบว่าวัฒนธรรมองค์กรมีบทบาทสำคัญในการสร้างแบบจำลองวัฒนธรรมความปลอดภัยทางไซเบอร์ที่เหมาะสม

3. เครื่องมือที่ใช้มากที่สุดในการประเมินวัฒนธรรมการรักษาความปลอดภัยในโลกไซเบอร์คือแบบสอบถามและแบบสำรวจ

Wajeb Gharibi and Maha Shaabi (2012) เรื่อง Cyber Threats in Social Networking Websites ศึกษาเรื่องภัยคุกคามทางไซเบอร์ในเครือข่ายสังคมออนไลน์ เว็บไซต์ โซเชียลออนไลน์ โดยการจำแนกประเภทภัยคุกคามทางไซเบอร์ แนะนำกลยุทธ์ต่อต้านภัยคุกคามและคาดการณ์แนวโน้มในอนาคตของเว็บไซต์ยอดนิยม แม้ว่าเว็บไซต์ เครือข่ายสังคมออนไลน์จะมีเทคโนโลยีขั้นสูงในการโต้ตอบและการสื่อสาร ซึ่งก่อให้เกิดความท้าทายใหม่ๆ เกี่ยวกับเรื่องความปลอดภัยของความเป็นส่วนตัว ได้สรุปว่า ความก้าวหน้าของเทคโนโลยีใหม่โดยทั่วไปและเว็บไซต์โซเชียลโดยเฉพาะ จะนำมาซึ่งความเสี่ยงด้านความปลอดภัยในรูปแบบใหม่ ๆ ที่อาจเปิดโอกาสสำหรับผู้มุ่งร้าย ดังนั้น ผู้เชี่ยวชาญด้านความปลอดภัยของข้อมูล ข้าราชการและหน่วยข่าวกรองอื่น ๆ ต้องพัฒนาเครื่องมือใหม่ที่ป้องกันและปรับให้เข้ากับความเสี่ยงและภัยคุกคามที่อาจเกิดขึ้นในอนาคต และสามารถจัดการกับข้อมูลในอินเทอร์เน็ตและในเว็บไซต์โซเชียลได้อย่างปลอดภัยด้วย

Miranda, Michael (2018) หัวข้อ Enhancing Cybersecurity Awareness Training: A Comprehensive Phishing Exercise Approach กล่าวว่า อีเมลเป็นเครื่องมือสื่อสารทางธุรกิจที่สำคัญ ดังนั้น อีเมลฟิชชิ่งที่หลอกลวงจะยังคงเป็นภัยคุกคามที่สำคัญต่อข้อมูลธุรกิจและผู้ใช้บริการและเทคโนโลยีสารสนเทศต่าง ๆ ด้วยการใช้โปรแกรมการฝึกฟิชชิ่งควบคู่ไปกับการรักษาความปลอดภัยของอีเมล โดยการใช้โปรแกรมการฝึกฟิชชิ่งที่มีโครงสร้างและครอบคลุม สามารถลดความน่าจะเป็นของความปลอดภัยทางไซเบอร์ที่เกิดจากอีเมลหลอกลวง และปรับปรุงความปลอดภัยทางไซเบอร์โดยรวม ความเสี่ยงที่เกี่ยวข้องกับภัยคุกคามนั้นสามารถบรรเทาลงได้อย่างสมเหตุสมผล เป้าหมายของโปรแกรมคือการทำได้มากกว่าเพียงแค่จับผู้ใช้ที่คลิกอีเมลปลอม การลดขนาดของกลุ่มผู้ใช้ในองค์กรส่วนน้อยที่มักจะถูกหลอกและตอบกลับอีเมลฟิชชิ่งเสมอ ดังนั้น เป้าหมายคือการฝึกอบรมฟิชชิ่งที่มีระเบียบ สม่ำเสมอ มีโครงสร้างและวัดผลได้

2.11 สรุป

ในบทที่ 2 นี้ เป็นการนำเสนอข้อมูลที่ได้ศึกษาแนวคิด ทฤษฎี เอกสารทางวิชาการ เพื่อเป็นข้อมูลในการดำเนินการวิจัย ประกอบด้วย แผนพัฒนาทักษะด้านดิจิทัลของข้าราชการกรุงเทพมหานครและบุคลากรกรุงเทพมหานคร เพื่อการปรับเปลี่ยนเป็นรัฐบาลดิจิทัล ระยะเริ่มแรก (Early) (พ.ศ. 2564 – 2565) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรฐานสากลที่เกี่ยวข้อง แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) แนวคิดเกี่ยวกับการคุกคามทางไซเบอร์

(Cyber Threat) แนวคิดด้านวัฒนธรรม แนวคิดเกี่ยวกับวัฒนธรรมองค์กร (Organizational Culture) แนวคิดเกี่ยวกับความรู้ (Knowledge) แนวคิดเกี่ยวกับความตระหนักรู้ (Awareness) และงานวิจัยที่เกี่ยวข้อง เพื่อนำมาเป็นแนวทางการในการวิเคราะห์ข้อมูลได้จากการดำเนินการวิจัยต่อไป

บทที่ 3

วิธีดำเนินการวิจัย

การวิจัยเรื่อง “การสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์” มีวัตถุประสงค์ 3 ข้อ ได้แก่ 1) เพื่อศึกษาพฤติกรรมและความพร้อมของบุคลากรที่มีต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ 2) เพื่อวิเคราะห์และสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ และ 3) เพื่อพัฒนาแอปพลิเคชันสำหรับประเมินวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ ซึ่งงานวิจัยนี้เป็นการวิจัยแบบผสมผสาน กล่าวคือเป็นการวิจัยเชิงคุณภาพ และการวิจัยเชิงปริมาณ โดยมีรายละเอียดดังต่อไปนี้

3.1 ศึกษาและรวบรวมข้อมูล ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

3.2 ประชากรและกลุ่มตัวอย่าง

3.3 การเก็บรวบรวมข้อมูล และเครื่องมือที่ใช้ในการวิจัย

3.4 การวิเคราะห์ข้อมูล

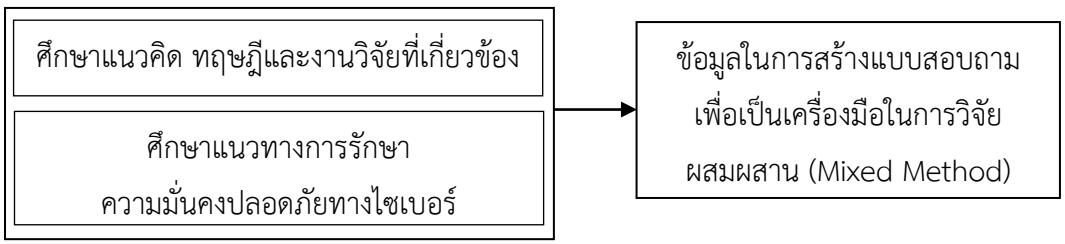
3.5 การวิเคราะห์ ออกแบบ และพัฒนาแอปพลิเคชัน

3.6 ระยะเวลาในการดำเนินงาน

3.7 สรุป

3.1 ศึกษาและรวบรวมข้อมูล ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ศึกษาและรวบรวมข้อมูล ทฤษฎีและงานวิจัยที่เกี่ยวข้อง เพื่อนำข้อมูลที่ได้มาเป็นข้อมูลในการสร้างเครื่องมือในการวิจัย ดังภาพประกอบที่ 3.1



ภาพประกอบที่ 3.1 ขั้นตอนการศึกษาและรวบรวมข้อมูล ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

จากการศึกษา แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง ที่ได้นำเสนอในบทที่ 2 ทำให้ทราบว่ากับการรักษามั่นคงปลอดภัยไซเบอร์นั้นไม่ใช่แค่การพัฒนาระบบเครือข่ายคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ให้พร้อมรับมือภัยคุกคามทางไซเบอร์ หากแต่ต้องเกิดจากความร่วมมือของบุคลากรในหน่วยงาน เพื่อลดโอกาสที่ระบบเครือข่ายคอมพิวเตอร์ขององค์กรจะเสียหายจากภัยคุกคามทางไซเบอร์ จำเป็นต้องทำให้บุคลากรมีความรู้ ความเข้าใจและความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ สอดคล้องกับแผนพัฒนาทักษะด้านดิจิทัลของข้าราชการกรุงเทพมหานครและบุคลากรกรุงเทพมหานคร เพื่อการปรับเปลี่ยนเป็นรัฐบาลดิจิทัล และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยผู้บริหารและผู้ดูแลระบบเครือข่ายองค์กรต้องมีการกำหนดขอบเขตและนโยบายการสร้างความมั่นคงปลอดภัยขององค์กรอย่างเข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยและเป็นแนวทางให้ทุกคนปฏิบัติตามได้ รวมทั้งเตรียมการรับมือและวางแผน ทั้งก่อนเกิด ขณะเกิดเหตุและหลังเกิดเหตุตามกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC27001 และ กรอบงาน NIST Cybersecurity Framework ซึ่งเป็นกรอบความมั่นคงปลอดภัยทางไซเบอร์ที่จะสนับสนุนการสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์เพื่อป้องกันการโจมตีทางไซเบอร์ ที่เปลี่ยนแปลงความคิดของผู้คนและพฤติกรรมของบุคคลให้เกิดความร่วมมือในการปฏิบัติที่ไปในทางเดียวกันจนเป็นการสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

3.2 ประชากรและกลุ่มตัวอย่าง

กำหนดบุคลากรในการเก็บรวบรวมข้อมูลในการวิจัย ดังนี้

3.2.1 บุคลากรผู้มีหน้าที่ในการดูแลและบริหารจัดการด้านระบบเครือข่ายหน่วยงาน ประกอบด้วย ผู้บริหารและผู้เชี่ยวชาญด้านระบบเครือข่ายของสารสนเทศกลางของหน่วยงานกรุงเทพมหานคร และ ผู้บริหารและผู้เชี่ยวชาญที่ปฏิบัติงานเกี่ยวข้องกับระบบเครือข่ายของสำนักการวางผังและพัฒนาเมือง เพื่อให้ทราบแนวทาง กรอบแนวคิดของผู้บริหารเกี่ยวกับการสร้างวัฒนธรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กร

3.2.2 บุคลากรผู้ใช้งานระบบเครือข่ายของสำนักการวางผังและพัฒนาเมือง เพื่อให้ทราบถึงพฤติกรรมและความพร้อมที่มีต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

บุคลากรที่ใช้ในการวิจัย ได้แก่ บุคลากรในสังกัดสำนักการวางผังและพัฒนาเมือง จำนวน 194 คน ผู้วิจัยได้ทำการสุ่มตัวอย่างของบุคลากรในหน่วยงาน จำนวน 131 คน โดยได้จากการคำนวณของสูตร ทาโร ยามาเน (Taro Yamane, 1973, น.125) ในการกำหนดตัวอย่าง โดยเลือกระดับความเชื่อมั่น 95% ค่าระดับความคลาดเคลื่อนยอมรับได้ไม่เกิน 5% หรือ 0.05 ของระดับนัยสำคัญ

การสุ่มตัวอย่างดังกล่าวของบุคลากรในหน่วยงานตามวิธีของ ยามาเน (Taro Yamane) ดังสมการที่ (3.1)

$$n = \frac{N}{1 + Ne^2} \quad (3.1)$$

เมื่อ n คือ ขนาดกลุ่มตัวอย่าง

N คือ ขนาดประชากร

e คือ ความคลาดเคลื่อนของกลุ่มตัวอย่าง เช่น

ระดับความเชื่อมั่น 90% สัดส่วนความคลาดเคลื่อนเท่ากับ 0.10

ระดับความเชื่อมั่น 95% สัดส่วนความคลาดเคลื่อนเท่ากับ 0.05

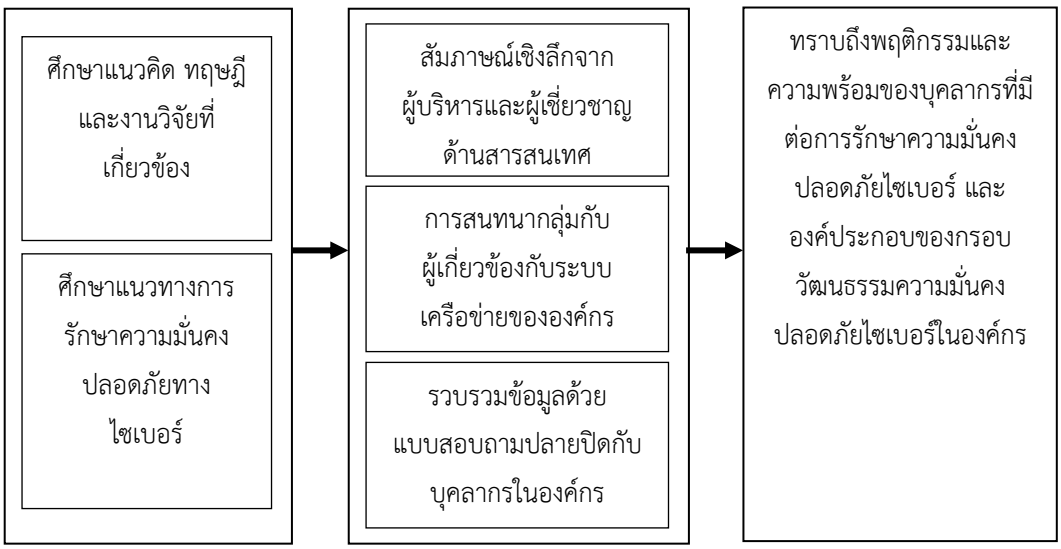
แทนค่าแทนค่าในสมการที่ 3.1 ได้เท่ากับ

n = 194 / (1+(194x0.05x0.05)) = 131

ขนาดกลุ่มตัวอย่าง จำนวน 131 คน

3.3 การเก็บรวบรวมข้อมูล เครื่องมือในการวิจัย

การสร้างเครื่องมือที่ใช้ในการวิจัยนี้เป็นการวิจัยแบบผสมผสาน โดยกำหนดแนวทางในการดำเนินการวิจัยให้สอดคล้องกับการศึกษาแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องในบทที่ 2 ดังภาพประกอบที่ 3.2



ภาพประกอบที่ 3.2 การเก็บรวบรวมข้อมูลและเครื่องมือในการวิจัย

3.3.1 การวิจัยเชิงคุณภาพ (Qualitative Research)

3.2.1.1 การสัมภาษณ์เชิงลึก (In-depth Interview) ผู้วิจัยสัมภาษณ์ด้วยตนเองด้วยการจดบันทึกจากการสัมภาษณ์ผู้บริหารและผู้เชี่ยวชาญด้านระบบเครือข่ายของสารสนเทศกลางของหน่วยงานกรุงเทพมหานคร และของสำนักการวางผังและพัฒนาเมือง จำนวน 15 คน

3.2.1.2 การสนทนากลุ่ม (Focus Group) ผู้วิจัยจัดการสนทนาแบบกลุ่มและบันทึกข้อมูลด้วยการจดบันทึกจากการสัมภาษณ์กับผู้ปฏิบัติงานเกี่ยวข้องกับระบบเครือข่ายของสำนักการวางผังและพัฒนาเมือง

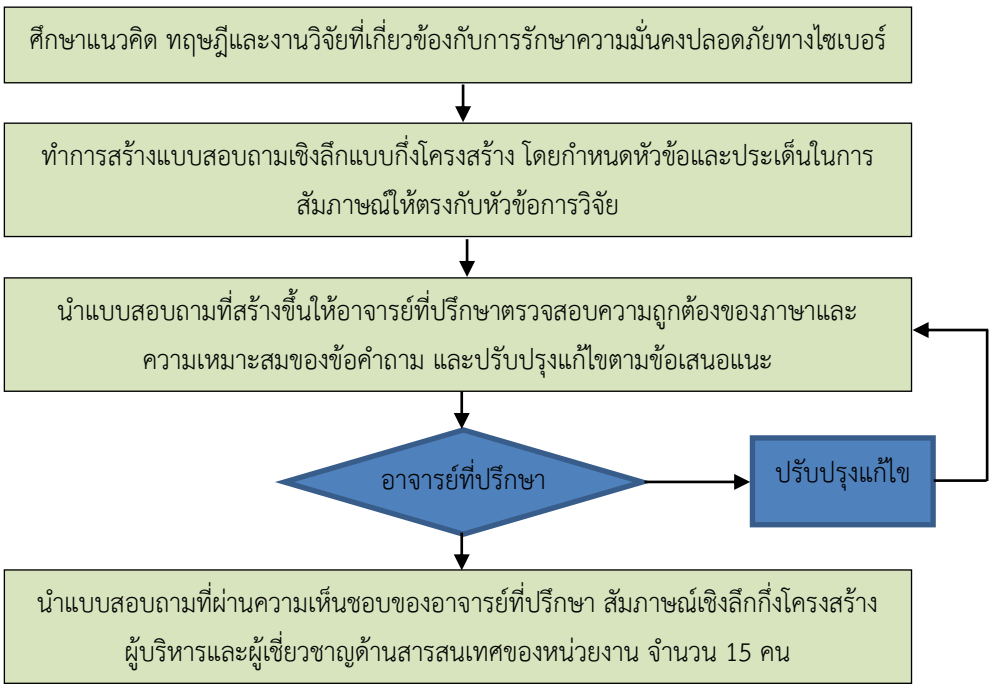
ข้อคำถามแบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 ข้อมูลส่วนบุคคลหรือหน่วยงานของผู้ตอบแบบสอบถาม

ส่วนที่ 2 ข้อคำถามเกี่ยวกับความคิดเห็นเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในองค์กร

ส่วนที่ 3 ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

3.2.1.3 การสร้างแบบสัมภาษณ์เชิงลึก (In-depth Interview) ผู้วิจัยได้สร้างแบบสัมภาษณ์จากการศึกษาเอกสารที่เกี่ยวข้องและกำหนดหัวข้อคำถามเสนออาจารย์ที่ปรึกษาเพื่อตรวจสอบความถูกต้องของภาษาและความเหมาะสมของข้อคำถาม และนำไปสัมภาษณ์ ดังแสดงในภาพประกอบ 3.3 (รายชื่อผู้ให้สัมภาษณ์แสดงในภาคผนวก ก)



ภาพประกอบที่ 3.3 แผนผังแสดงขั้นตอนการสร้างแบบสัมภาษณ์เชิงลึก

3.2.2 การวิจัยเชิงปริมาณ : แบบสอบถามปลายปิด

การใช้แบบสอบถามออนไลน์ช่วยในการเก็บข้อมูล และดำเนินการเก็บรวบรวมข้อมูลจากแบบสอบถามออนไลน์และตรวจสอบความสมบูรณ์ของการกรอกแบบสอบถาม

โดยให้กลุ่มตัวอย่างที่กำหนดไว้เป็นผู้ตอบคำถามเอง (Self-Administered) คำถามแบ่งออกเป็นส่วน ๆ ดังนี้

ส่วนที่ 1 : ข้อมูลส่วนบุคคลหรือหน่วยงานของผู้ตอบแบบสอบถาม

ส่วนที่ 2 : ข้อคำถามเกี่ยวกับความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ส่วนที่ 3 : ข้อคำถามเกี่ยวกับพฤติกรรมเสี่ยงต่อภัยคุกคามต่อระบบเครือข่ายของหน่วยงาน

การกำหนดเกณฑ์การให้คะแนนแบบสอบถาม

ลักษณะคำตอบของแบบสอบถามในส่วนที่ 2 และ 3 เป็นลักษณะของการใช้มาตราส่วนประเมินค่า (Rating Scale) ของลิเคิร์ท (Likert Scale) ซึ่งเป็นมาตรวัดชนิดประมาณค่าจากค่าน้อยที่สุดถึงค่ามากที่สุด มาตรวัดแบบประมาณค่า คือ การวัดแบบจัดอันดับ ชนิด 5 ระดับ โดยมีระยะห่างระหว่างแต่ละจุดของสเกลจะมีค่าเท่ากัน โดยมีเกณฑ์ดังนี้

ระดับความคิดเห็น	**คะแนน**
เห็นด้วยมากที่สุด	5
เห็นด้วยมาก	4
เห็นด้วยปานกลาง	3
เห็นด้วยน้อย	2
เห็นด้วยน้อยที่สุด	1

จากนั้นคำนวณหาค่าพิสัยเพื่อจัดระยะห่างของช่วงชั้นออกเป็น 5 ระดับคือ ตามสมการที่ (3.2) ดังนี้

$$\text{อันตรภาคชั้น} = \frac{\text{พิสัย}}{\text{จำนวนชั้น}} = \frac{\text{คะแนนสูงสุด} - \text{คะแนนต่ำสุด}}{\text{จำนวนชั้น}} \quad (3.2)$$

$$\text{แทนค่าในสมการที่ 3.2} = \frac{5 - 1}{5}$$

$$= 0.8$$

จากการพิจารณาอันตรภาคชั้นของช่วงระดับคะแนน สามารถกำหนดระดับคะแนนเพื่อใช้ในการแปลผล ดังนี้

ค่าเฉลี่ย 4.21 – 5.00 หมายถึง เห็นด้วยมากที่สุด

ค่าเฉลี่ย 3.21 – 4.20 หมายถึง เห็นมาก

ค่าเฉลี่ย 2.61 – 3.40 หมายถึง เห็นด้วยปานกลาง

ค่าเฉลี่ย 1.81 – 2.60 หมายถึง เห็นด้วยน้อย

ค่าเฉลี่ย 1.00 – 1.80 หมายถึง เห็นด้วยน้อยที่สุด

3.2.3 การตรวจสอบคุณภาพของแบบสอบถาม

3.2.3.1 การคัดเลือกกลุ่มผู้เชี่ยวชาญ ผู้วิจัยได้จัดทำเกณฑ์การคัดเลือกผู้เชี่ยวชาญในการพิจารณาคุณภาพของแบบสอบถาม จำนวน 5 คน ดังนี้

- มีวุฒิทางการศึกษาระดับไม่ต่ำกว่าปริญญาโท ด้านเทคโนโลยีสารสนเทศหรือทางคอมพิวเตอร์
- เคยทำวิจัยในเรื่องที่เกี่ยวกับด้านเทคโนโลยีสารสนเทศ
- เป็นวิทยากรหรือสอนในวิชาด้านเทคโนโลยีสารสนเทศ
- มีความรู้ ความสามารถและประสบการณ์ทางด้านสถิติ

3.2.3.2 ตรวจสอบค่าความเที่ยงตรง (Validity) เป็นตรวจสอบความถูกต้องในเนื้อหา (Content Validity) ว่าคุณสมบัติของข้อคำถามที่สามารถวัดได้ตรงตามเนื้อหาและพฤติกรรมที่ต้องการวัดหรือไม่ แล้วก็ตรวจสอบค่าความเที่ยงตรงเชิงโครงสร้าง (Construct Validity) และตรวจสอบค่าความเที่ยงตรงตามเกณฑ์ที่เกี่ยวข้อง โดยนำแบบสอบถามไปให้ผู้ทรงคุณวุฒิตรวจสอบความเที่ยงตรงเพื่อวิเคราะห์หาค่าดัชนีความสอดคล้อง (Index of Item Objective Congruence : IOC) ดังนี้

1. แน่ใจว่ามีความสอดคล้องหรือวัดได้ มีระดับคะแนนเท่ากับ 1
2. ไม่แน่ใจว่ามีความสอดคล้องหรือวัดได้ มีระดับคะแนนเท่ากับ 0
3. แน่ใจว่าไม่มีความสอดคล้องหรือวัดได้ มีระดับคะแนนเท่ากับ -1

หลังจากนั้นนำแบบประเมินโมเดลให้ผู้ทรงคุณวุฒิประเมินความสอดคล้องของข้อคำถามกับวัตถุประสงค์ และนำมาหาค่าความสอดคล้องโดยใช้สูตร ตามสมการที่ (3.3) ดังนี้

$$IOC = \frac{\Sigma R}{N} \qquad (3.3)$$

R หมายถึง ผลคูณของคะแนนกับจำนวนผู้เชียวชาญ

N หมายถึง จำนวนผู้เชี่ยวชาญ

ในการพิจารณาความคิดเห็นของผู้เชี่ยวชาญ จากการหาค่าดัชนีความสอดคล้อง (IOC) ในทุกข้อคำถามนั้น มีค่าเท่ากับ 1.00 หากข้อคำถามที่มีค่า IOC ตั้งแต่ 0.50 - 1.00 จะคัดเลือกไว้ ส่วนข้อคำถามที่มีค่า IOC ต่ำกว่า 0.50 จะนำมาพิจารณาปรับปรุงข้อคำถามใหม่ หรือจะตัดทิ้งก็ได้ตามความเหมาะสม ซึ่งได้รับความอนุเคราะห์จากผู้เชี่ยวชาญช่วยตรวจสอบเครื่องมือวิจัยประกอบด้วย 5 ท่าน ดังนี้

1. อาจารย์ สำราญ ไชยคำวัง
2. อาจารย์ บุญชม สุดจิตต์
3. นายเกรียงไกร ภูวณิชย์
4. นายเทพฤทธิ์ พระเทพ
5. นางสาววิรัลพัชร พรหมจรรย์

จากการหาค่าดัชนีความสอดคล้อง (IOC) จากผู้ทรงคุณวุฒิจำนวน 5 ท่าน พบว่ามีข้อคำถามมีค่า IOC ตั้งแต่ 0.60 – 1.00 จึงได้นำแบบสอบถามกระจายไปให้กลุ่มตัวอย่างได้ทำแบบสอบถามต่อไป

3.2.3.3 ตรวจสอบค่าความเชื่อมั่น (Reliability) ของแบบสอบถาม ผู้วิจัยจะทำการทดสอบ (Pre-Test) กับกลุ่มตัวอย่าง จำนวน 30 คน เพื่อทดสอบความเชื่อมั่นของแบบสอบถาม การทดสอบหาค่าความเชื่อมั่นของแบบสอบถาม โดยวิธีหาค่าสัมประสิทธิ์แอลฟ่าของคอนบัค (Cronbach’s alpha coefficient) ด้วยโปรแกรม SPSS ดังสมการที่ (3.4) ดังนี้

$$\alpha = \frac{n}{n-1}\left(1 - \frac{\Sigma S_i^2}{S_t^2}\right) \qquad (3.4)$$

โดย α คือ ค่าสัมประสิทธิ์ความเชื่อมั่นของแบบสอบถาม

n คือ จำนวนข้อคำถามในแบบสอบถาม

ΣS_i^2 คือ ผลร่วมของความแปรปรวนของแบบสอบถามรายข้อ

S_t^2 คือ ความแปรปรวนของแบบสอบถามทั้งฉบับ

ซึ่งค่า α ต้องมีค่ามากกว่า 0.7 ขึ้นไป

ตารางที่ 3.1 แสดงค่าความเชื่อมั่น (Reliability) ของแบบสอบถาม

ตัวแปร	จำนวนข้อคำถาม	ค่า Cronbach's Alpha
ด้านความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยไซเบอร์ Cognition (COG)	6 ข้อ	0.801
ด้านพฤติกรรมการใช้อินเทอร์เน็ต Internet (INT)	5 ข้อ	0.900
ด้านพฤติกรรมการใช้งานสื่อสังคม Social (SOC)	3 ข้อ	0.827
ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์ On-Line (ONL)	4 ข้อ	0.933
ด้านพฤติกรรมการใช้งานผ่านโปรแกรม Program (PRO)	4 ข้อ	0.907
ด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต Cybersecurity Treats (CST)	4 ข้อ	0.876

จากตารางที่ 3.1 แสดงค่าความเชื่อมั่น (Reliability) พบว่า ข้อคำถามด้านความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัย ไซเบอร์ จำนวน 6 ข้อ มีค่า Cronbach's Alpha เท่ากับ .801 ข้อคำถามด้านพฤติกรรมการใช้อินเทอร์เน็ต Internet จำนวน 5 ข้อ มีค่า Cronbach's Alpha เท่ากับ .900 ข้อคำถามด้านพฤติกรรมการใช้งานสื่อสังคม Social จำนวน 3 ข้อ มีค่า Cronbach's Alpha เท่ากับ .827 ข้อคำถามด้านพฤติกรรมการเข้าถึงสื่อออนไลน์ On-Line จำนวน 4 ข้อ มีค่า Cronbach's Alpha เท่ากับ .933 ข้อคำถามด้านพฤติกรรมการใช้งานผ่านโปรแกรม Program จำนวน 4 ข้อ มีค่า Cronbach's Alpha เท่ากับ .907 และข้อคำถามด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต Cybersecurity Treats จำนวน 6 ข้อ มีค่า Cronbach's Alpha เท่ากับ .876 ซึ่งข้อคำถามทั้ง 6 ด้าน มีค่า Cronbach's Alpha มากกว่า 0.7 ดังนั้น แบบสอบถาม ได้ค่ามีความน่าเชื่อถือ (Reliability) จึงนำไปใช้เป็นเครื่องมือในการเก็บรวบรวมข้อมูลต่อไป

3.2.3 อุปกรณ์ที่ใช้ในการวิจัย

3.2.3.1 ฮาร์ดแวร์ คือเครื่องคอมพิวเตอร์โน๊ตบุ๊ค

3.2.3.3 ซอฟต์แวร์ คือโปรแกรม Microsoft office word โปรแกรม SPSS

3.4 การวิเคราะห์ข้อมูล

3.4.1 การวิเคราะห์ข้อมูลการสัมภาษณ์เชิงลึกและการสนทนากลุ่ม จะใช้การสรุปประเด็นสำคัญจากผู้ให้ข้อมูลที่มีประสบการณ์ในการทำงานด้านเทคโนโลยีดิจิทัลหรือทำงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และนำข้อมูลมาเปรียบเทียบเพื่อหาข้อสรุป

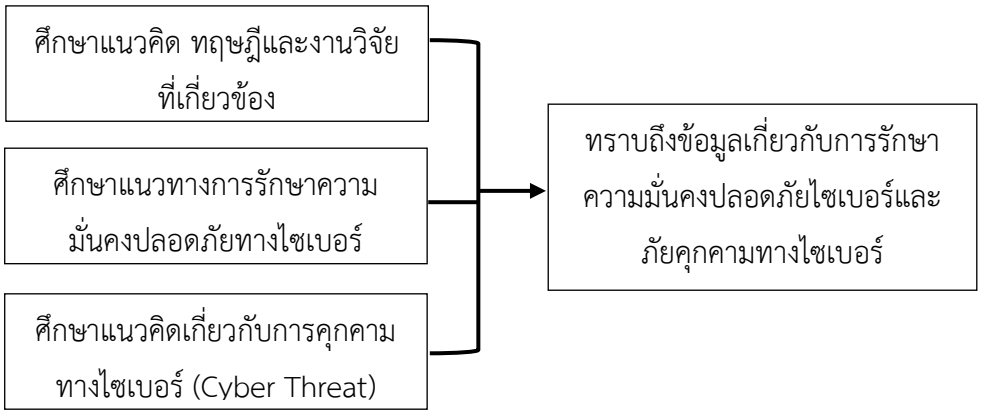
3.4.2 การวิเคราะห์ข้อมูลการสัมภาษณ์เชิงลึกและการสนทนากลุ่ม จะใช้การสรุปประเด็นสำคัญจากผู้ให้ข้อมูลที่มีประสบการณ์ในการทำงานด้านเทคโนโลยีดิจิทัลหรือทำงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และนำข้อมูลมาเปรียบเทียบเพื่อหาข้อสรุป

3.5 การวิเคราะห์ ออกแบบและพัฒนาแอปพลิเคชัน

การดำเนินการตามวัตถุประสงค์ข้อที่ 3 เพื่อพัฒนาแอปพลิเคชันสำหรับประเมินวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ ผู้วิจัยจึงได้พัฒนาแอพพลิเคชั่นโดยใช้วงจรการพัฒนาระบบงาน (Software Development Life Cycle : SDLC) ดังนี้

3.5.1 การกำหนดปัญหา (Requirement Definition)

3.5.1.1 ศึกษา แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้องเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทำให้ทราบถึงข้อมลเกี่ยวกับแนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์และภัยคุกคามทางไซเบอร์ ดังภาพประกอบที่ 3.4



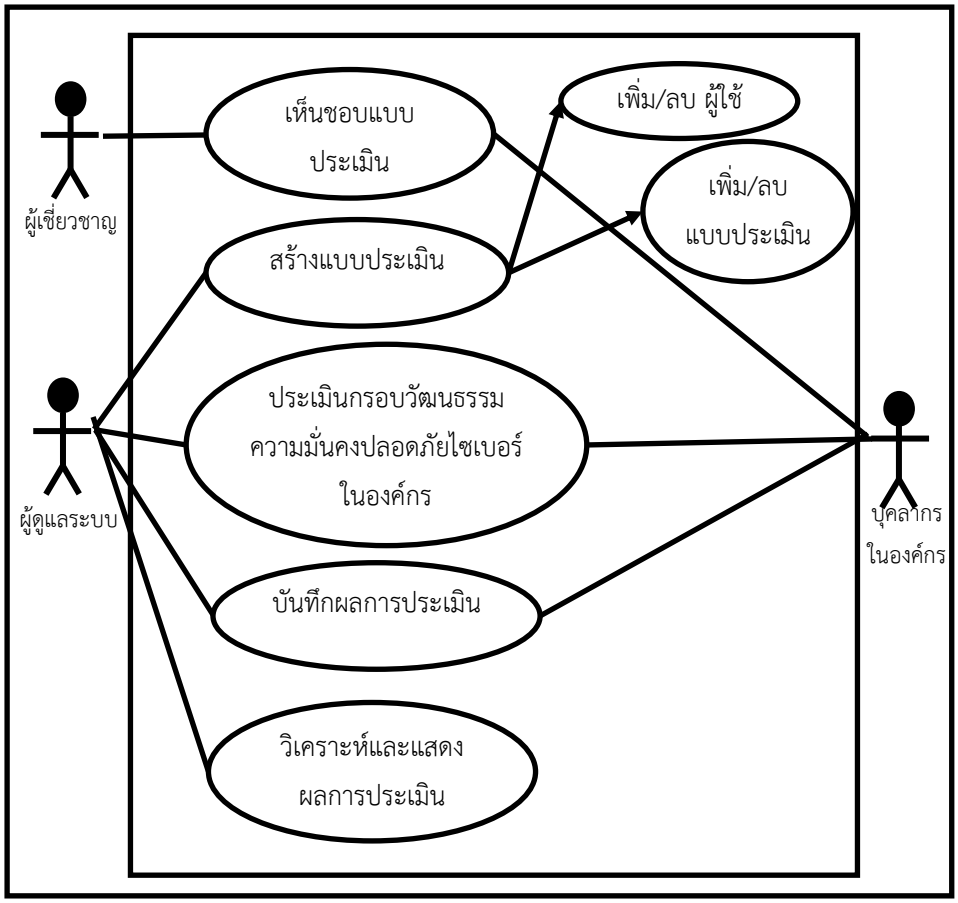
ภาพประกอบที่ 3.4 ขั้นตอนการศึกษาข้อมูลเพื่อกำหนดปัญหา

3.5.1.2 ทำการศึกษาและวิเคราะห์ภัยคุกคามทางไซเบอร์และแนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยการสัมภาษณ์เชิงลึกกับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ และการสนทนากลุ่ม (Focus Group) กับผู้ปฏิบัติงานเกี่ยวข้องกับระบบเครือข่าย

3.5.1.3 แบบสอบถามปลายปิดสำหรับการวิจัยเชิงปริมาณ จากการศึกษาและวิเคราะห์ภัยคุกคามทางไซเบอร์และแนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และจากการสัมภาษณ์เชิงลึกกับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ และการสนทนากลุ่ม (Focus Group) กับผู้ปฏิบัติงานเกี่ยวข้องกับระบบเครือข่าย แบ่งคำถามออกเป็น 5 ส่วน

3.5.2 การวิเคราะห์ปัญหา (Analysis) นำเอาสิ่งที่ได้จากขั้นตอนแรกมาทำการวิเคราะห์เพื่อเตรียมความพร้อมในการออกแบบแอปพลิเคชันสำหรับประเมินวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร

3.5.3 การออกแบบ (Design) จะเป็นการนำเอาสิ่งที่ได้จากการวิเคราะห์มาออกแบบเป็นระบบงานสำหรับการพัฒนาในขั้นตอนถัดไป ดังภาพประกอบที่ 3.5



ภาพประกอบที่ 3.5 แสดงแผนภาพ Use Case Diagram ของแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร

3.5.4 การพัฒนาระบบงาน (Development) พัฒนาแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร เพื่อให้มีความง่ายต่อการใช้งานและสอดคล้องกับข้อมูลในการประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร ดังภาพประกอบที่ 3.6

ภาพประกอบที่ 3.6 การออกแบบหน้าจอแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร

3.5.5 การทดสอบ (Testing) การทดสอบระบบตรวจสอบความถูกต้องของระบบงานที่ถูกสร้างขึ้นมาว่าตรงตามกับความต้องการจริงๆ หรือไม่ ก่อนที่จะดำเนินการติดตั้งระบบเพื่อใช้งานจริง โดยผู้วิจัยได้ให้ผู้ปฏิบัติงานเกี่ยวข้องกับระบบเครือข่ายทดสอบการทำแบบประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรในแอปพลิเคชัน Intention to Use Cyber Insurance

3.5.6 การติดตั้ง (Implementation) ขั้นตอนการนำแอปพลิเคชันไปใช้งานจริง เมื่อทำการทดสอบตามข้อ 3.5.5 เรียบร้อยแล้ว

3.5.7 การบำรุงรักษา (Maintenance) เป็นการปรับปรุงแก้ไขแอปพลิเคชันให้เหมาะสมกับการใช้งานจริง และปรับปรุงข้อมูลให้มีความเหมาะสมต่อองค์กรต่อไป

3.6 ระยะเวลาในการดำเนินงาน

ตารางที่ 3.2 ระยะเวลาในการดำเนินงานวิจัย

ขั้นตอนการดำเนินงาน	ระยะเวลาในการดำเนินการศึกษา ปี พ.ศ. 2564 – 2565											
	ปี พ.ศ. 2564				ปี พ.ศ. 2565							
	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.
1.ศึกษาแนวคิด ทฤษฎีต่าง ๆ และทบทวนวรรณกรรมที่เกี่ยวข้อง												
2.นำเสนอหัวข้อและจัดทำเอกสารบทที่ 1 - 3												
3.วิเคราะห์และพัฒนากรอบแนวคิดการวิจัย												
4.รวบรวมข้อมูลและการวิเคราะห์ข้อมูล												
5.ออกแบบและพัฒนาแอปพลิเคชันสำหรับประเมินฯ												
6.ทดสอบและปรับปรุงแอปพลิเคชัน												
7.สรุปและอภิปรายผล												
8.จัดทำบทความวิชาการ เพื่อนำเสนอในการประชุมวิชาการ												

ตารางที่ 3.2 ระยะเวลาในการดำเนินงานวิจัย (ต่อ)

ขั้นตอนการดำเนินงาน	ระยะเวลาในการดำเนินการศึกษา ปี พ.ศ. 2564 – 2565											
	ปี พ.ศ. 2564				ปี พ.ศ. 2565							
	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.
9.จัดทำเอกสารบทที่ 4 – 5 ภาคผนวกและเรียบเรียงสารนิพนธ์ฉบับสมบูรณ์ตามรูปแบบที่บัณฑิตวิทยาลัยกำหนด												
10.นำเสนองานในการประชุมวิชาการ												
11.นำเสนอผลงานต่อคณะกรรมการสอบและนำส่งเล่มฉบับสมบูรณ์												
12.ปรับปรุงแก้ไขหลังการนำเสนอ												

3.7 สรุป

ในบทที่ 3 นี้เป็นการเสนอระเบียบวิธีวิจัยเป็นขั้นตอนในการวิจัย ซึ่งประกอบด้วยการศึกษาและรวบรวมข้อมูล ทฤษฎีและงานวิจัยที่เกี่ยวข้อง กำหนดประชากรและกลุ่มตัวอย่าง เครื่องมือที่ใช้ในการวิจัย การวิเคราะห์ข้อมูล การวิเคราะห์ ออกแบบ และพัฒนาแอปพลิเคชัน รวมทั้งระยะเวลาในการดำเนินงาน เพื่อตอบคำถามตามวัตถุประสงค์และสมมติฐานที่กำหนดไว้ ซึ่งผู้วิจัยจะนำเสนอผลการวิเคราะห์ผลการวิจัยในบทที่ 4 ต่อไป

บทที่ 4

ผลการวิจัย

การศึกษาและวิจัยในครั้งนี้เป็นการสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์” โดยผู้วิจัยมีวัตถุประสงค์ 3 ข้อ ได้แก่

1. เพื่อศึกษาพฤติกรรมและความพร้อมของบุคลากรที่มีต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

2. เพื่อวิเคราะห์และสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

3. เพื่อพัฒนาแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

โดยในบทนี้ จะได้นำเสนอผลการวิจัยตามลำดับของวัตถุประสงค์ทั้ง 3 ข้อที่ได้ดำเนินการศึกษาและวิจัย ดังต่อไปนี้

4.1 ผลการวิจัยตามวัตถุประสงค์ ข้อที่ 1

ผลการศึกษาและวิจัย เพื่อให้สามารถตอบวัตถุประสงค์ข้อที่ 1 ผู้วิจัยได้ทำการศึกษาโดยใช้เครื่องมือคือ แบบสอบถามเพื่อเก็บรวบรวมข้อมูล โดยใช้แบบสอบถาม ดังนี้

4.1.1 การวิจัยเชิงคุณภาพ (Qualitative Research) โดยการสัมภาษณ์เชิงลึก (In-depth Interview) กับผู้เชี่ยวชาญด้านระบบเครือข่ายของสารสนเทศกลางของหน่วยงานกรุงเทพมหานครและกลุ่มงานสารสนเทศของสำนักการวางผังและพัฒนาเมือง จำนวน 15 คน และการสนทนากลุ่ม (Focus Group) กับผู้ปฏิบัติงานเกี่ยวข้องกับระบบเครือข่ายของสำนักการวางผังและพัฒนาเมือง ได้ข้อสรุป ดังตารางที่ 4.1

ตารางที่ 4.1 สรุปผลการวิเคราะห์เนื้อหาจากการสัมภาษณ์เชิงลึกและการสนทนากลุ่ม

คำถามในการสัมภาษณ์	ข้อมูลจากการสัมภาษณ์เชิงลึก
ในปัจจุบันปัญหาและอุปสรรคด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กร เป็นอย่างไร	1.บุคลากร แบ่งเป็น 2 กลุ่ม คือ กลุ่มผู้ใช้งานทั่วไป และกลุ่มผู้ดูแลระบบยังขาดความรู้ ความเข้าใจในเรื่องความมั่นคงปลอดภัยไซเบอร์ รวมทั้งไม่รู้กฎหมาย ระเบียบที่เกี่ยวข้อง 2. โครงสร้างพื้นฐาน ระบบที่ใช้ในการดูแลด้านความมั่นคงปลอดภัย ขาดงบประมาณในการสนับสนุนในการบริการจัดการอุปกรณ์ ไม่ทันต่อเทคโนโลยีของภัยคุกคามทางไซเบอร์ 3. โครงสร้างของกรุงเทพมหานคร การกำหนดนโยบาย มาตรฐาน แนวทางในการปฏิบัติจากผู้บริหาร/ส่วนกลางยังไม่มีความชัดเจน
ความพร้อมด้านความมั่นคงปลอดภัยในองค์กรเป็นอย่างไร	1. ด้านบุคลากร มีความพร้อมในระดับการเรียนรู้ แต่ยังขาดความรู้เชิงป้องกัน/การเตรียมความพร้อมในการรับมือ 2. ด้านระบบ (System) มีความพร้อมทางด้านอุปกรณ์อยู่ในระดับปานกลาง ยังไม่ Update เท่าทันเทคโนโลยีและภัยคุกคามทางไซเบอร์ใหม่ ๆ
มีปัจจัยอะไรที่จะทำให้การรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กรประสบความสำเร็จ	1. ด้านบุคลากร การคุกคามทางไซเบอร์มีการเข้าถึงอุปกรณ์ได้ตลอดเวลา ผู้ใช้งานต้องมีการใช้งานด้วยความระมัดระวัง และมีความรู้ในการใช้งานของอุปกรณ์ในการป้องกันการคุกคามจะเป็นปัจจัยหลักในการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กรได้ 2. ด้านระบบการบริหารจัดการ ผู้ดูแลระบบต้องมีความเข้าใจถึงผลกระทบในการเกิดภัยคุกคามทางไซเบอร์ 3. ด้านการบริหาร ควรมีการกำหนดนโยบาย การบริหารงบประมาณในการพัฒนาทั้งด้านระบบและบุคลากร

ตารางที่ 4.1 สรุปผลการวิเคราะห์เนื้อหาจากการสัมภาษณ์เชิงลึกและการสนทนากลุ่ม (ต่อ)

คำถามในการสัมภาษณ์	ข้อมูลจากการสัมภาษณ์เชิงลึก
จากคำตอบข้างต้น ควรมีการส่งเสริมหรือปรับปรุงในแต่ละปัจจัยอย่างไร	1. ด้านบุคลากร ส่งเสริมการสร้างความรู้ ความเข้าใจและความตระหนักรู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ให้ทันสมัยอยู่เสมอ 2. ด้านระบบจัดการโครงสร้าง ควรครอบคลุมและเชื่อมโยงได้อย่างมีประสิทธิภาพระหว่างหน่วยงานต่าง ๆ ของ กทม. 3. ด้านการบริหาร มีการกำหนดนโยบาย แนวทางมาตรฐานที่ชัดเจนจากหน่วยงานกลางไปยังหน่วยงานในสังกัด กทม. (สวพ.) ต่อไป
การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ มีความสำคัญอย่างไร	การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์มีความสำคัญมาก การใช้งานระบบดิจิทัลที่มีข้อมูลจำนวนมากและ มีมูลค่า และการบริการข้อมูล หากมีปัญหาและไม่สามารถแก้ไขได้ทันท่วงทีจะมีผลกระทบต่อข้อมูลและการให้บริการ การป้องกันที่ดีคือ การสร้างความตระหนักรู้ถึงความมั่นคงปลอดภัยไซเบอร์ขององค์กร บุคลากรให้ความร่วมมือกับองค์กร ปฏิบัติตามระเบียบและแนวปฏิบัติในด้านความมั่นคงปลอดภัยทางไซเบอร์
ความคิดเห็นหรือข้อเสนอแนะเกี่ยวกับการสร้างกรอบหรือองค์ประกอบการสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กร	การสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ คือ บุคลากร โดยการสร้างความรู้ ความเข้าใจและสำนึกความรับผิดชอบให้กับบุคลากร ดังนี้ 1. ผู้บริหาร กำหนดนโยบาย/แนวทางในการปฏิบัติให้กับบุคลากรจัดสรรงบประมาณในการจัดการระบบให้มีเทคโนโลยีที่ทันสมัย 2. ผู้ดูแลระบบ ศึกษาระเบียบ ข้อกฎหมายต่าง ๆ และผลกระทบที่อาจเกิดจากภัยคุกคามทางไซเบอร์ นำเสนอผู้บริหารเพื่อกำหนดเป็นนโยบาย/แนวทางในการปฏิบัติต่อไป 3. ผู้ใช้งานทั่วไป สร้างความรู้ ความเข้าใจ และความตระหนักถึงผลกระทบจากภัยคุกคามทางไซเบอร์

จากตารางที่ 4.1 พบว่า การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรมีความสำคัญมาก การใช้งานระบบดิจิทัลที่มีข้อมูลจำนวนมากและข้อมูลมีมูลค่า และการให้บริการข้อมูลต่าง ๆ หากระบบมีปัญหาและไม่สามารถแก้ไขได้ทันท่วงที ย่อมจะมีผลกระทบต่อข้อมูลและการให้บริการ การป้องกันที่ดี คือ การสร้างความตระหนักรู้ถึงความมั่นคงปลอดภัยไซเบอร์ขององค์กร สร้างความรู้ ความเข้าใจและสำนึกความรับผิดชอบให้กับบุคลากร ดังนี้

1. ผู้บริหาร กำหนดนโยบาย/แนวทางในการปฏิบัติให้กับบุคลากรจัดสรรงบประมาณในการจัดการระบบให้มีเทคโนโลยีที่ทันสมัย

2. ผู้ดูแลระบบ ศึกษาระเบียบ ข้อกฎหมายต่าง ๆ และผลกระทบที่อาจเกิดจากภัยคุกคามทางไซเบอร์ นำเสนอผู้บริหารเพื่อกำหนดเป็นนโยบาย/แนวทางในการปฏิบัติต่อไป

3. ผู้ใช้งานทั่วไป สร้างความรู้ ความเข้าใจ และความตระหนักถึงผลกระทบจากภัยคุกคามทางไซเบอร์

4.1.2 การวิจัยเชิงปริมาณ โดยใช้เครื่องมือที่เป็นแบบสอบถามปลายปิด ทำการสำรวจจากกลุ่มตัวอย่างที่เป็นบุคลากรของสำนักการวางผังและพัฒนาเมือง เกี่ยวกับความรู้ ความเข้าใจ และพฤติกรรมในการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กร รายละเอียดแสดงไว้ในตารางที่ 4.2

ตารางที่ 4.2 สรุปผลการประเมินพฤติกรรมในการรักษาความมั่นคงปลอดภัยของบุคลากรในองค์กร

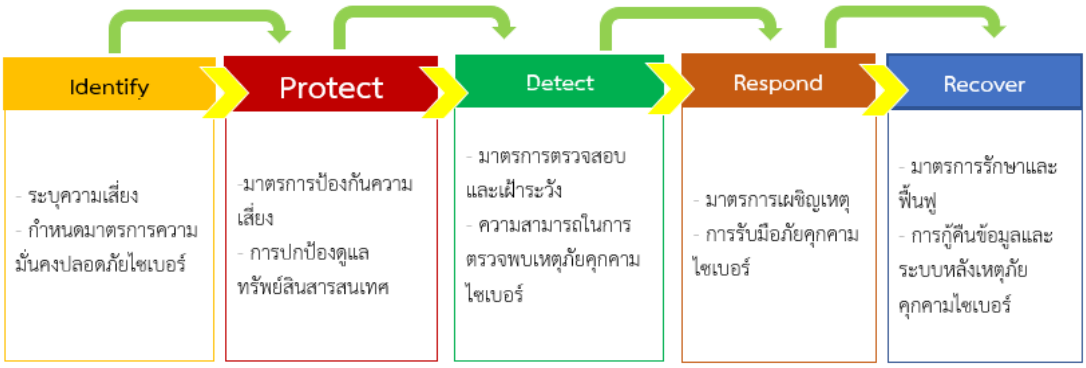
รายการประเมิน	$\bar{X}$	**S.D.**	**แปลผล**
1. ด้านความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยทางไซเบอร์	4.38	0.68	มากที่สุด
2. ด้านพฤติกรรมเสี่ยงต่อภัยคุกคามต่อระบบเครือข่ายของหน่วยงาน			
2.1 ด้านพฤติกรรมการใช้อินเทอร์เน็ต	3.98	0.48	มาก
2.2 ด้านพฤติกรรมการใช้งานสื่อสังคม	3.55	0.32	ปานกลาง
2.3 ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์	4.18	0.39	มาก
2.4 ด้านพฤติกรรมการใช้งานผ่านโปรแกรม	4.00	0.42	มาก
2.5 ด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต	3.62	0.33	ปานกลาง
ระดับความคิดเห็นเฉลี่ยโดยรวม	**3.95**	**0.44**	**มาก**

จากตารางที่ 4.2 ผลการประเมินพฤติกรรมการใช้งานระบบเครือข่ายในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในสำนักการวางผังและพัฒนาเมือง ในแต่ละด้านมีค่าเฉลี่ยปานกลางถึงมากที่สุด ที่ใกล้เคียงกัน ทำให้โดยภาพรวมอยู่ในระดับมาก

4.2 ผลการวิเคราะห์ข้อมูลตามวัตถุประสงค์ ข้อที่ 2

จากการศึกษาแนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ในบทที่ 2 ประกอบกับข้อมูลที่ได้จากการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้างและการสนทนากลุ่มตามตารางที่ 4.1 และข้อมูลผลการประเมินพฤติกรรมบุคลากรในองค์ในด้านรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในองค์กร ตามตารางที่ 4.2 พบว่า กรอบงาน NIST Cybersecurity Framework เป็นกรอบความมั่นคงปลอดภัยทางไซเบอร์ที่จะสนับสนุนการสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ขององค์กร และนำกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC27001 มาเป็นแนวทางในการดำเนินการเพื่อสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ขององค์กร สรุปปัจจัยที่มีผลต่อการสร้างความมั่นคงปลอดภัยไซเบอร์ของสำนักการวางผังและพัฒนาเมืองได้ ดังนี้

1. กรอบงาน NIST Cybersecurity Framework กรอบความมั่นคงปลอดภัยทางไซเบอร์ที่จะสนับสนุนการสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ รายละเอียดดังภาพประกอบที่ 4.1



ภาพประกอบที่ 4.1 กรอบงาน NIST Cybersecurity Framework ขององค์กร

2. มาตรฐาน ISO/IEC27001 ซึ่งเป็นมาตรฐานการจัดการข้อมูลที่สำคัญ มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร ประกอบด้วย 4 ขั้นตอนหลัก PDCA (Plan - Do - Check - Action) รายละเอียดดังตารางที่ 4.3

ตารางที่ 4.3 ผลการวิเคราะห์ข้อมูลตามวัตถุประสงค์ ข้อที่ 2 ตามมาตรฐาน ISO/IEC27001

ขั้นตอน	ปัจจัย
1. การวางแผน (Plan)	ปัจจัยที่ 1 นโยบายด้านความมั่นคงปลอดภัยไซเบอร์ ที่ระบุว่าองค์กรต้องมีการกำหนดนโยบายและขั้นตอนในการปฏิบัติที่ชัดเจนจากผู้บริหารระดับสูง

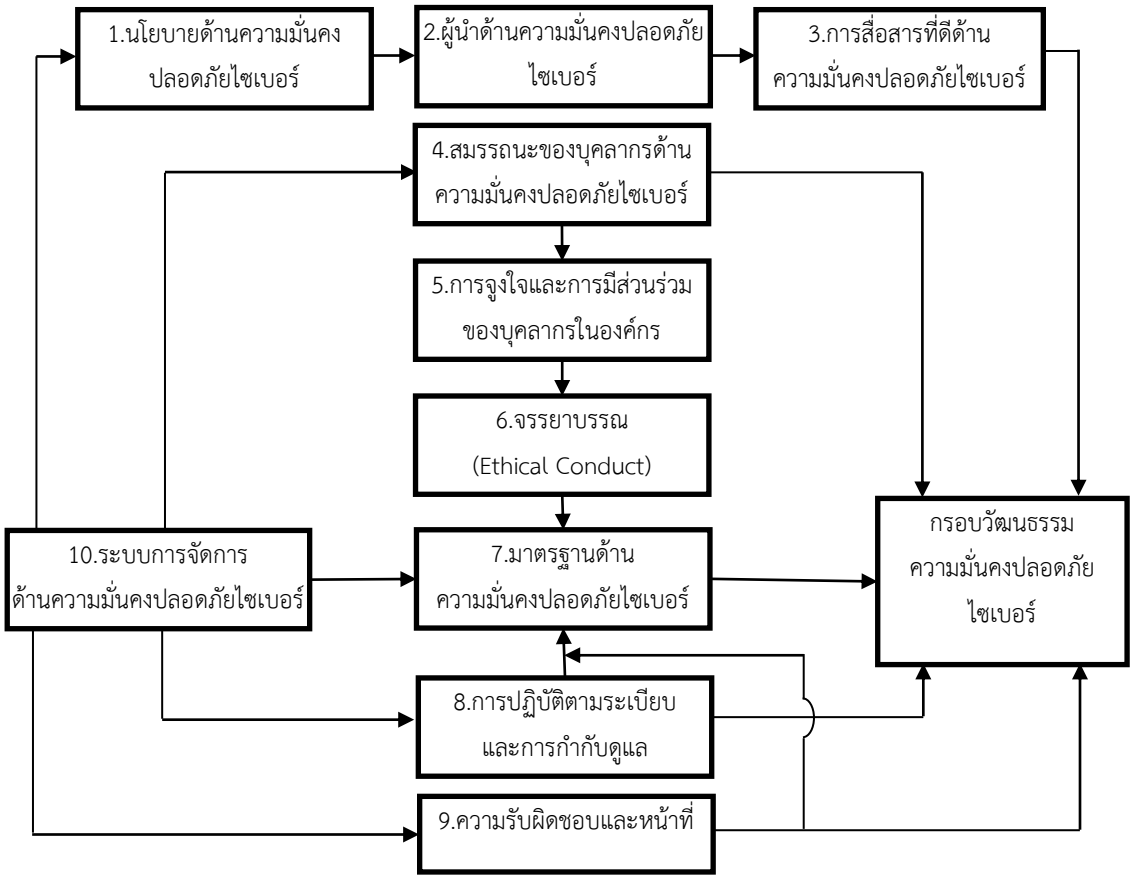
ตารางที่ 4.3 ผลการวิเคราะห์ข้อมูลตามวัตถุประสงค์ ข้อที่ 2 ตามมาตรฐาน ISO/IEC27001

ขั้นตอน	ปัจจัย
1. การวางแผน (Plan)	ปัจจัยที่ 2 ผู้นำด้านความมั่นคงปลอดภัยไซเบอร์ ผู้บริหารจะต้องมีการกำหนดนโยบายที่ชัดเจนแล้ว จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ สนับสนุนการสร้างความตระหนักรู้และการกำกับดูแลการใช้งานระบบเครือข่าย และประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์
	ปัจจัยที่ 3 การสื่อสารที่ดีด้านความมั่นคงปลอดภัยไซเบอร์ มีการเผยแพร่แนวทางในการปฏิบัติ แผนการรับมือภัยคุกคามทางไซเบอร์ และมีแนวทางให้บุคลากรได้เรียนรู้ประสบการณ์ด้านไซเบอร์ในองค์กรร่วมกัน
2. การปฏิบัติตาม (Do)	ปัจจัยที่ 4 สมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ บุคลากรในองค์กรได้รับการฝึกอบรมด้านความมั่นคงปลอดภัย สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัย สามารถถ่ายทอดความรู้ระหว่างกันในองค์กรได้
	ปัจจัยที่ 5 การจูงใจและการมีส่วนร่วมของบุคลากรในองค์กร องค์กรสร้างความเชื่อมั่นและวางใจในระบบเครือข่ายขององค์กร ว่ามีเครื่องมือหรืออุปกรณ์ในองค์กรที่อำนวยความสะดวกในการทำงานอย่างมีประสิทธิภาพ ทำให้บุคลากรมีความพร้อมในการร่วมมือด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ขององค์กร ซึ่งสอดคล้องกับงานวิจัยของ Kabanda, Gabriel ที่พบว่า การเปลี่ยนแปลงความคิดและพฤติกรรมของผู้คนเป็นไฟร์วอลล์ของมนุษย์ที่แข็งแกร่งในการต่อต้านภัยคุกคามทางไซเบอร์
	ปัจจัยที่ 6 จรรยาบรรณ (Ethical Conduct) การใช้งานระบบดิจิทัลที่มีข้อมูลจำนวนมากและมีมูลค่า องค์กรต้องมีการกำหนดแนวทางในการปกปิดข้อมูลส่วนบุคคล การรักษาความถูกต้องของข้อมูล และการทำลายข้อมูล ก่อนที่จะเกิดผลกระทบต่อข้อมูลและการให้บริการ
3. การตรวจสอบ (Check)	ปัจจัยที่ 7 มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ องค์กรต้องมีการตรวจสอบระบบเครือข่ายอย่างสม่ำเสมอ การจัดเก็บข้อมูลจราจร (Log) และกระบวนการควบคุมการใช้งานอุปกรณ์ในการเชื่อมต่อระบบเครือข่ายขององค์กร

ตารางที่ 4.3 ผลการวิเคราะห์ข้อมูลตามวัตถุประสงค์ ข้อที่ 2 ตามมาตรฐาน ISO/IEC27001 (ต่อ)

ขั้นตอน	ปัจจัย
3. การตรวจสอบ (Check)	ปัจจัยที่ 8 การปฏิบัติตามระเบียบและการกำกับดูแล กำหนดสิทธิ หน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูลของแต่ละส่วนงาน กระบวนการตรวจสอบและประเมินคุณภาพของข้อมูลได้
	ปัจจัยที่ 9 ความรับผิดชอบและหน้าที่ กำหนดหน้าที่ความรับผิดชอบของบุคลากรในองค์กร กำหนดขั้นตอนและซักซ้อมการแก้ไขปัญหา
4. ปรับปรุงแก้ไข (Action)	ปัจจัยที่ 10 ระบบการจัดการด้านความมั่นคงปลอดภัยไซเบอร์ แนวทางในการป้องกันและแก้ไขปัญหาการบุกรุกระบบเครือข่าย สร้างระบบยืนยันตัวตน และระบบจัดเก็บข้อมูลให้อยู่ในสถานะที่มีความปลอดภัย

จากตารางที่ 4.3 สามารถสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์สำหรับสำนักการวางผังและพัฒนาเมือง กรุงเทพมหานคร ได้ดังภาพประกอบที่ 4.2



ภาพประกอบที่ 4.2 กรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร

ผลการประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ ที่ประกอบด้วยปัจจัย 10 ด้าน ได้แสดงไว้ในตารางที่ 4.4

ตารางที่ 4.4 ผลการประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

รายการประเมิน	**ระดับความคิดเห็นของผู้เชี่ยวชาญ**		
	$\bar{X}$	**S.D.**	**แปลผล**
1. ความเหมาะสมของกรอบวัฒนธรรมฯ	3.80	0.45	มาก
2. การยอมรับของกรอบวัฒนธรรมฯ	4.20	0.45	มาก
ระดับความคิดเห็นเฉลี่ยโดยรวม	**4.00**	**0.45**	**มาก**

จากตารางที่ 4.4 แสดงผลการประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์จากผู้บริหารองค์กร พบว่า ความเหมาะสมของกรอบวัฒนธรรมฯ มีค่าอยู่ในระดับมาก ($\bar{X}$= 3.80) และการยอมรับของกรอบวัฒนธรรมฯ มีค่าอยู่ในระดับมาก ($\bar{X}$= 4.20)

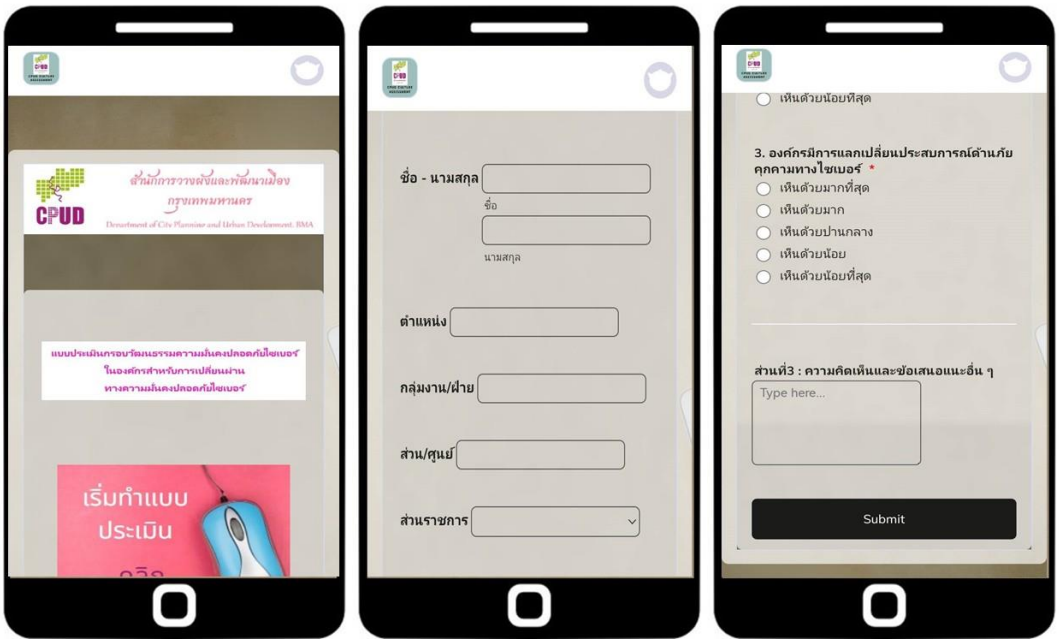
4.3 ผลการวิเคราะห์ข้อมูลตามวัตถุประสงค์ ข้อที่ 3

จากผลการวิเคราะห์ข้อมูลตามวัตถุประสงค์ ข้อที่ 1 และ ข้อที่ 2 นำข้อมูลที่ได้มาพัฒนาแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ ด้วย Jotform.com โดยแอปพลิเคชันมีชื่อว่า “CPUD Culture Assessment” ติดตั้งแอปพลิเคชันผ่านทาง QR CODE ดังภาพประกอบที่ 4.3

ภาพประกอบที่ 4.3 QR CODE .ติดตั้งแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงไซเบอร์

แอปพลิเคชันจะให้เลือกติดตั้งแอปพลิเคชัน และแสดง Icon แอปพลิเคชัน ดังภาพประกอบที่ 4.4 และเมื่อติดตั้งสำเร็จ สามารถทำการประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงไซเบอร์ได้ตามหน้าแอปพลิเคชันที่พร้อมใช้งาน ดังภาพประกอบที่ 4.5

ภาพประกอบที่ 4.4 ภาพการเลือกติดตั้งแอปพลิเคชันและ Icon แอปพลิเคชันเมื่อติดตั้งสำเร็จ



ภาพประกอบที่ 4.5 ภาพหน้าจอแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงไซเบอร์

จากการนำแอปพลิเคชันให้บุคลากรในองค์กรทำแบบประเมินวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ ของสำนักการวางผังและพัฒนาเมือง กรุงเทพมหานคร แล้ว ได้ผลการประเมิน ดังนี้

4.3.1 ข้อมูลส่วนบุคคลหรือหน่วยงานของผู้ตอบแบบสอบถาม

ตารางที่ 4.5 แสดงจำนวนและค่าร้อยละของข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

รายการประเมิน	จำนวน (คน)	ร้อยละ
เพศ		
1. ชาย	26	32.50
2. หญิง	54	67.50
อายุ		
1. ต่ำกว่า 30 ปี	3	3.75
2. 30 – 40 ปี	35	43.75
3. 41 – 50 ปี	27	33.75
4. 51 – 60 ปี	15	18.75
ระดับการศึกษา		
1. ต่ำกว่าปริญญาตรี	10	12.5
2. ปริญญาตรี	33	41.25
3. ปริญญาโท	37	46.25
4. ปริญญาเอก	-	-
สายงานที่ปฏิบัติ		
1. ด้านบริหาร	10	12.50
2. ด้านปฏิบัติการ	47	58.75
3. ด้านธุรการ	12	15.00
4. ด้านอื่น ๆ	11	13.75
ระยะเวลาในการปฏิบัติงานในหน่วยงาน		
1. ไม่เกิน 5 ปี	31	38.75
2. 6 – 10 ปี	20	25.00
3. 11 – 15 ปี	2	2.50
4. 16 ปี ขึ้นไป	27	33.75
รวม	**80**	**100.00**

4.3.2 ข้อมูลการประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร 10 ปัจจัย

ตารางที่ 4.6 สรุปผลการประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร

รายการประเมิน	$\bar{X}$	**S.D.**	**แปลผล**
ปัจจัยที่ 1 นโยบายด้านความมั่นคงปลอดภัยไซเบอร์			
1. องค์กรมีการกำหนดแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	4.62	0.64	มากที่สุด
2. องค์กรมีการกำหนดหน้าที่ของบุคลากรที่กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์	4.61	0.69	มากที่สุด
3. องค์กรมีการกำหนดระดับสิทธิในการเข้าถึงระบบเครือข่ายของหน่วยงาน	4.59	0.73	มากที่สุด
4. องค์กรมีการกำหนดให้มีการบำรุงรักษาหรือซ่อมแซมอุปกรณ์คอมพิวเตอร์ซึ่งดำเนินการโดยบุคลากรที่ได้รับอนุญาต	4.66	0.67	มากที่สุด
ระดับความคิดเห็นเฉลี่ยโดยรวม	4.62	0.68	มากที่สุด
ปัจจัยที่ 2 ผู้นำด้านความมั่นคงปลอดภัยไซเบอร์			
1. องค์กรมีการจัดทำแผนรับมือภัยคุกคามทาง ไซเบอร์	4.43	0.65	มาก
2. องค์กรมีการสนับสนุนการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์	4.45	0.74	มาก
3. องค์กรมีการกำกับดูแลการใช้งานระบบเครือข่ายให้เป็นไปตามแนวทางปฏิบัติของหน่วยงาน	4.43	0.73	มาก
4. องค์กรมีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยไซเบอร์	4.40	0.78	มาก
ระดับความคิดเห็นเฉลี่ยโดยรวม	4.43	0.73	มากที่สุด

ตารางที่ 4.6 สรุปผลการประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร (ต่อ)

รายการประเมิน	$\bar{X}$	S.D.	แปลผล
ปัจจัยที่ 3 การสื่อสารที่ดีด้านความมั่นคงปลอดภัยไซเบอร์			
1. องค์กรมีการเผยแพร่นโยบายและแนวปฏิบัติให้บุคลากรในหน่วยงานได้รับทราบและปฏิบัติ	4.49	0.59	มาก
2. องค์กรมีการเผยแพร่แผนการรับมือภัยคุกคามทางไซเบอร์	4.55	0.62	มากที่สุด
3. องค์กรมีการเผยแพร่ความรู้ด้านการรับมือภัยคุกคามทางไซเบอร์	4.47	0.67	มาก
4. องค์กรมีแนวทางให้บุคลากรได้เรียนรู้ประสบการณ์ด้านไซเบอร์ร่วมกัน	4.44	0.69	มาก
ระดับความคิดเห็นเฉลี่ยโดยรวม	4.49	0.64	มากที่สุด
ปัจจัยที่ 4 สมรรถนะของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์			
1. องค์กรมีการการฝึกอบรมสร้างความตระหนักรู้ด้านความปลอดภัย	4.54	0.56	มากที่สุด
2. องค์กรมีการการสนับสนุนบุคลากรในการพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์	4.50	0.65	มากที่สุด
3. บุคลากรสามารถถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยระหว่างกันในองค์กร	4.50	0.65	มากที่สุด
4. บุคลากรมี Cyber Mindset และ Cyber Ethics	4.55	0.59	มากที่สุด
ระดับความคิดเห็นเฉลี่ยโดยรวม	4.52	0.61	มากที่สุด

ตารางที่ 4.6 สรุปผลการประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร (ต่อ)

รายการประเมิน	$\bar{X}$	S.D.	แปลผล
ปัจจัยที่ 5 การจูงใจและการมีส่วนร่วมของบุคลากรในองค์กร			
1. บุคลากรมีความเชื่อมั่นในมาตรการปกป้องข้อมูลส่วนบุคคลในองค์กร	4.57	0.62	มากที่สุด
2. บุคลากรมีความไว้วางใจในระบบเครือข่ายขององค์กร	4.44	0.69	มาก
3. องค์กรมีอุปกรณ์ในสำนักงานที่สามารถอำนวยความสะดวกในการทำงานได้อย่างมีประสิทธิภาพ	4.65	0.69	มากที่สุด
4. บุคลากรมีความพร้อมและให้ความร่วมมือในการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กร	4.38	0.65	มากที่สุด
ระดับความคิดเห็นเฉลี่ยโดยรวม	4.51	0.66	มากที่สุด
ปัจจัยที่ 6 จรรยาบรรณ (Ethical Conduct)			
1. องค์กรมีการกำหนดวิธีรักษาและทำลายข้อมูลขององค์กร	4.39	0.77	มากที่สุด
2. องค์กรมีแนวทางการดำเนินการปกปิดข้อมูลส่วนบุคคล	4.22	0.62	มากที่สุด
3. องค์กรมีแนวปฏิบัติในการรักษาความสมบูรณ์ถูกต้องของข้อมูล	4.55	0.62	มากที่สุด
ระดับความคิดเห็นเฉลี่ยโดยรวม	4.39	0.67	มากที่สุด

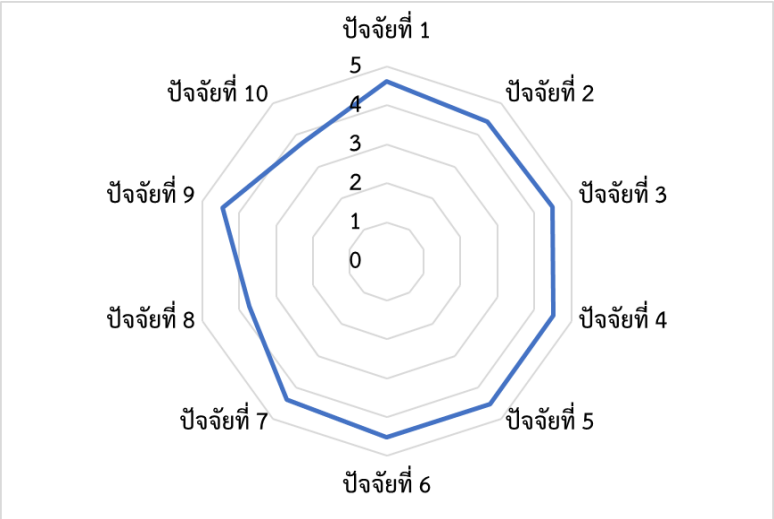
ตารางที่ 4.6 สรุปผลการประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร (ต่อ)

รายการประเมิน	$\bar{X}$	S.D.	แปลผล
ปัจจัยที่ 7 มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์			
1. องค์กรมีการตรวจสอบภายในด้าน (IT Audit)	4.55	0.59	มากที่สุด
2. องค์กรมีการการจัดเก็บข้อมูลจราจร (Log)	4.54	0.58	มากที่สุด
3. องค์กรมีการกำหนดสิทธิระบบเครือข่ายไร้สายให้กับบุคคลภายในและภายนอก	4.52	0.64	มากที่สุด
4. องค์กรมีกระบวนการควบคุมการใช้งานอุปกรณ์ส่วนตัวที่มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์	4.55	0.62	มากที่สุด
ระดับความคิดเห็นเฉลี่ยโดยรวม	4.54	0.61	มากที่สุด
ปัจจัยที่ 8 การปฏิบัติตามระเบียบและการกำกับดูแล (Compliance and Governance)			
1. องค์กรมีการกำหนดสิทธิ หน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูลของแต่ละส่วนงาน	4.52	0.60	มากที่สุด
2. องค์กรมีการกำหนดนโยบาย/กฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูล	4.44	0.59	มากที่สุด
3. องค์กรมีการกำหนดมาตรการหรือกระบวนการตรวจสอบและประเมินคุณภาพข้อมูล	4.49	0.59	มากที่สุด
4. องค์กรมีมาตรฐานสากลในการบริหารจัดการข้อมูล	4.33	0.65	มากที่สุด
ระดับความคิดเห็นเฉลี่ยโดยรวม	4.45	0.61	มากที่สุด

ตารางที่ 4.6 สรุปผลการประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร (ต่อ)

รายการประเมิน	$\bar{X}$	S.D.	แปลผล
ปัจจัยที่ 9 ความรับผิดชอบและหน้าที่ (Accountability and Responsibility)			
1. องค์กรมีการกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของบุคลากรในหน่วยงาน	4.22	0.55	มากที่สุด
2. องค์กรมีการระบุขั้นตอนและซักซ้อมการแก้ไขปัญหาการบุกรุกระบบเครือข่ายคอมพิวเตอร์	4.00	0.48	มาก
3. องค์กรมีการแลกเปลี่ยนประสบการณ์ด้านภัยคุกคามทางไซเบอร์	3.02	0.44	ปานกลาง
ระดับความคิดเห็นเฉลี่ยโดยรวม	3.75	0.49	มาก
ปัจจัยที่ 10 ระบบการจัดการด้านความมั่นคงปลอดภัยไซเบอร์			
1. ระบบเครือข่ายขององค์กรมีระบบการยืนยันตัวตน	4.39	0.77	มากที่สุด
2. องค์กรมีการกำหนดสิทธิและระดับในการเข้าถึงข้อมูลหรือระบบต่าง ๆ ของบุคลากร	4.22	0.62	มากที่สุด
3. องค์กรมีระบบจัดเก็บและถ่ายโอนข้อมูลสารสนเทศให้อยู่ในสถานะที่มีความปลอดภัย	4.55	0.62	มากที่สุด
4. องค์กรมีแนวทางการป้องกันและแก้ไขปัญหาการบุกรุกระบบเครือข่าย	4.44	0.72	มากที่สุด
ระดับความคิดเห็นเฉลี่ยโดยรวม	4.40	0.68	มากที่สุด
ระดับความคิดเห็นเฉลี่ยโดยรวมทั้ง 10 ปัจจัย	**4.41**	**0.64**	**มากที่สุด**

จากตารางพบว่าภาพรวมของแต่ละปัจจัยอยู่ในระดับมากที่สุด ปัจจัยที่มีค่าประเมินเฉลี่ยสูงสุดคือ ปัจจัยที่ 1 นโยบายด้านความมั่นคงปลอดภัยไซเบอร์ มีค่าอยู่ในระดับมากที่สุด ($\bar{X}$= 4.62) และปัจจัยที่มีค่าประเมินต่ำสุดคือ ปัจจัยที่ 9 ความรับผิดชอบและหน้าที่ มีค่าอยู่ในระดับมาก ($\bar{X}$= 3.75) ดังภาพประกอบที่ 4.6



ภาพประกอบที่ 4.6 ผลการประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงไซเบอร์

ผลการประเมินแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ ได้แสดงไว้ในตารางที่ 4.7

ตารางที่ 4.7 ผลการประเมินแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

รายการประเมิน	**ระดับความคิดเห็นของผู้เชี่ยวชาญ**		
	$\bar{X}$	**S.D.**	**แปลผล**
1. ความเหมาะสมของแอปพลิเคชันฯ	4.40	0.52	มากที่สุด
2. การยอมรับของแอปพลิเคชันฯ	4.40	0.52	มากที่สุด
ระดับความคิดเห็นเฉลี่ยโดยรวม	**4.40**	**0.52**	**มากที่สุด**

จากตารางที่ 4.5 แสดงผลการประเมินแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ พบว่าความเหมาะสมของแอปพลิเคชันฯ มีค่าอยู่ในระดับมาก ($\bar{X}$= 4.40) และการยอมรับของแอปพลิเคชันฯ มีค่าอยู่ในระดับมาก ($\bar{X}$= 0.52)

4.4 ผลการวิจัยเพื่อตอบสมมติฐาน

สมมติฐานข้อที่ 1 ความพร้อมของบุคลากรในองค์กรที่มีต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ มีค่าอยู่ในระดับมาก

จากผลการวิจัยพบว่า การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรมีความสำคัญมาก โดยการป้องกันที่ดี คือ การสร้างความตระหนักรู้ถึงความมั่นคงปลอดภัยไซเบอร์ขององค์กร สร้างความรู้ ความเข้าใจและสำนึกความรับผิดชอบให้กับบุคลากร และผลการประเมินพฤติกรรมการใช้งานระบบเครือข่ายในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในสำนักการวางผังและพัฒนาเมือง ในแต่ละด้านมีค่าเฉลี่ยปานกลางถึงมากที่สุด ที่ใกล้เคียงกัน ทำให้โดยภาพรวมอยู่ในระดับมาก ซึ่งเป็นไปตามสมมติฐานข้อที่ 1 นั่นคือ ความพร้อมของบุคลากรในองค์กรที่มีต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ มีค่าอยู่ในระดับมาก ($\overline{X}$= 3.95)

สมมติฐานข้อที่ 2 กรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ มีความเหมาะสมอยู่ในระดับมาก

จากผลการวิจัยพบว่า ผลการประเมินกรอบกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ ที่ประกอบด้วยปัจจัย 10 ด้าน สำหรับสำนักการวางผังและพัฒนาเมือง กรุงเทพมหานคร มีความเหมาะสมอยู่ในระดับมาก ซึ่งเป็นไปตามสมมติฐานข้อที่ 2 นั่นคือ กรอบกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ทางความมั่นคงปลอดภัยไซเบอร์ มีความเหมาะสมอยู่ในระดับมาก ($\overline{X}$= 3.80)

สมมติฐานข้อที่ 3 กรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ มีการยอมรับอยู่ในระดับมาก

จากผลการวิจัยพบว่า ผลการประเมินกรอบกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ ที่ประกอบด้วยปัจจัย 10 ด้าน สำหรับสำนักการวางผังและพัฒนาเมือง กรุงเทพมหานคร มีการยอมรับอยู่ในระดับมาก ซึ่งเป็นไปตามสมมติฐานข้อที่ 3 นั่นคือ กรอบกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ทางความมั่นคงปลอดภัยไซเบอร์ มีการยอมรับอยู่ในระดับมาก ($\overline{X}$= 4.20)

4.5 สรุป

ในบทที่ 4 นี้เป็นการเสนอผลการวิเคราะห์ข้อมูลตามวัตถุประสงค์การวิจัย ทั้ง 3 ข้อ ได้แก่ 1) ผลการวิเคราะห์ข้อมูลตามวัตถุประสงค์ข้อที่ 1 เพื่อศึกษาพฤติกรรมและความพร้อมของบุคลากรที่มีต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ 2) ผลการวิเคราะห์ข้อมูลตามวัตถุประสงค์ข้อที่ 2 เพื่อวิเคราะห์และสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ และ 3) ผลการวิเคราะห์ข้อมูลตามวัตถุประสงค์ข้อที่ 3 เพื่อพัฒนาแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ ซึ่งผู้วิจัยสรุปผลการวิจัยเพื่อตอบสมมติฐานการวิจัย อภิปรายผล และข้อเสนอแนะในบทที่ 5 ต่อไป

บทที่ 5

สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

จากการศึกษาและวิจัย เรื่อง “การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์” มีวัตถุประสงค์ 1) เพื่อศึกษาพฤติกรรมและความพร้อมของบุคลากรที่มีต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ 2) เพื่อวิเคราะห์และสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ และ 3) เพื่อพัฒนาแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ โดยสามารถสรุปผลการวิจัยเป็น 3 ส่วนได้ดังนี้

5.1 สรุปผลการวิจัย

5.2 อภิปรายผล

5.3 ปัญหา อุปสรรคและข้อจำกัดของการวิจัย

5.4 ข้อเสนอแนะ

5.1 สรุปผลการวิจัย

การวิจัยเรื่อง “การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์” เป็นการวิจัยแบบผสมผสาน กล่าวคือเป็นการวิจัยเชิงคุณภาพ โดยการสัมภาษณ์เชิงลึก การสนทนากลุ่ม และการวิจัยเชิงปริมาณ ผลการวิจัยพบว่า การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ของสำนักการวางผังและพัฒนาเมือง จะต้องเกิดจากการมีส่วนร่วมของบุคลากรในทุกระดับที่สอดคล้องไปในแนวทางเดียวกัน คือ ระดับผู้บริหารองค์กรต้องกำหนดนโยบายและแนวทางการปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจน ปฏิบัติตามแนวทางที่กำหนดเพื่อเป็นแบบอย่างให้ผู้ใต้บังคับบัญชา และสนับสนุนการบริหารจัดการทั้งในการจัดการระบบและการพัฒนาบุคลากร ระดับผู้ดูแลระบบ ต้องพัฒนาทักษะในการดูแลระบบการจัดการด้านความมั่นคงปลอดภัยไซเบอร์ และการสื่อสารที่ดีต่อบุคลากรในระดับอื่น ๆระดับผู้ใช้งานทั่วไป ต้องพัฒนาทักษะ

ด้านความมั่นคงปลอดภัยไซเบอร์ให้มีความรู้ ความเข้าใจ และความตระหนักถึงภัยคุกคามทางไซเบอร์ และปฏิบัติตามแนวทางที่ได้กำหนดไว้ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และพัฒนาแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ของสำนักการวางผังและพัฒนาเมือง

5.2 อภิปรายผล

จากการศึกษาแนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ ประกอบกับข้อมูลที่ได้จากการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้าง การสนทนากลุ่มและข้อมูลผลการประเมินพฤติกรรมบุคลากรในองค์ในด้านรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในองค์กร พบว่า

การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ของสำนักการวางผังและพัฒนาเมือง กรุงเทพมหานคร โดยการนำหลักการกรอบงาน NIST Cybersecurity Framework เป็นกรอบความมั่นคงปลอดภัยทางไซเบอร์ที่จะสนับสนุนการสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ขององค์กร และกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC27001 เป็นแนวทางในการดำเนินการเพื่อสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ขององค์กร จะได้ปัจจัยที่มีผลต่อการสร้างความมั่นคงปลอดภัยไซเบอร์ของสำนักการวางผังและพัฒนาเมือง 10 ด้าน ประกอบด้วย 3 องค์ประกอบหลักคือ ผู้บริหาร บุคลากรและระบบการจัดการ กล่าวคือ จะต้องเกิดจากการมีส่วนร่วมของบุคลากรในทุกระดับที่สอดคล้องในแนวทางเดียวกันจึงจะเกิดการสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร สอดคล้องกันกับงานวิจัยของ Kabanda, Gabriel. (2561) ได้ศึกษาเรื่อง A Cybersecurity Culture Framework and Its Impact on Zimbabwean Organizations พบว่า กรอบงาน NIST Cybersecurity Framework เป็นสิ่งที่จะสนับสนุนวัฒนธรรมความปลอดภัยทางไซเบอร์เพื่อป้องกันการโจมตีทางไซเบอร์ ที่เปลี่ยนแปลงความคิดของผู้คนและพฤติกรรมของบุคคลให้เป็นไฟร์วอลล์ที่แข็งแกร่งในการต่อต้านภัยคุกคามทางไซเบอร์ได้โดยไม่มีการบังคับและเป็นตามกรอบที่สถาบันมาตรฐานและเทคโนโลยีแห่งชาติสร้างขึ้น และงานวิจัยของ กริน ธัญญวิกรม และ ธีระ กุลสวัสดิ์ (2564) ที่ได้ศึกษาการจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ กรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย ที่มีข้อเสนอแนะว่าในการรักษาความมั่นคงปลอดภัยไซเบอร์ ควรมีนโยบายที่สำคัญ ดังนี้ 1) รัฐควรเร่งรัดการบังคับกฎหมายและประกาศกฎเกณฑ์ต่าง ๆ เพื่อให้การดำเนินการมีความสอดคล้องและเป็นไปในทิศทางเดียว 2) ธนาคารควรส่งเสริมให้ความรู้และตะหนักถึงภัยคุกคามไซเบอร์ และภัยคุกคามทางการเงินในการทำธุรกรรมการเงินทางอิเล็กทรอนิกส์ให้กับประชาชนและลูกค้าของธนาคารให้มากขึ้น และ 3)

ภาคประชาชนควรจะเรียนรู้และตระหนักถึงภัยคุกคามไซเบอร์ภัยคุกคามทางการเงินในการทำธุรกรรมการเงินทางอิเล็กทรอนิกส์

5.3 ปัญหา อุปสรรคและข้อจำกัดของการวิจัย

การวิจัยเรื่อง “การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์” ผู้วิจัยพบว่า มีปัญหา อุปสรรคและข้อจำกัดของการวิจัย ดังนี้

1. ในการทำงานวิจัยเรื่องนี้ มีข้อจำกัดด้านระยะเวลาในการค้นคว้า ทบทวนวรรณกรรม ซึ่งหากมีเวลามากในการค้นคว้ามากขึ้น จะได้ศึกษาเอกสารที่เกี่ยวข้องกับงานวิจัยให้ได้จำนวนมากขึ้น ทำให้มีความเข้าใจในหัวข้อวิจัยและประเด็นที่เกี่ยวข้องกับงานวิจัยมากขึ้น แต่ด้วยผู้วิจัยมีการทำงานประจำที่มักจะมีงานที่ต้องทำนอกเวลาด้วย จึงทำให้ต้องบริหารจัดการเวลาให้สามารถดำเนินงานวิจัยให้แล้วเสร็จ

2. การพัฒนาแอปพลิเคชันสำหรับประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ของสำนักการวางผังและพัฒนาเมืองที่สามารถประเมินผลได้ ยังต้องมีการศึกษาข้อมูลและปรับปรุงแก้ไขให้เหมาะสมกับบริบทขององค์กรในภายหน้า

5.4 ข้อเสนอแนะ

งานวิจัยนี้เป็นการศึกษา การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ของสำนักการวางผังและพัฒนาเมืองกรุงเทพมหานคร และพัฒนาแอปพลิเคชันเพื่อประเมินกรอบการสร้างวัฒนธรรมดังกล่าว ซึ่งเป็นการเก็บข้อมูลจากกลุ่มตัวอย่างขององค์กรเท่านั้น ดังนั้นในการวิจัยครั้งต่อไปจึงเสนอแนะ ดังนี้

1. ควรมีการศึกษาและเก็บข้อมูลกับบุคลากรในองค์กรทั้งหมด เพื่อให้ทราบผลการประเมินที่ครอบคลุมและนำข้อมูลที่ได้มาเป็นเครื่องมือที่ทำให้องค์กรทราบผลการประเมินในแต่ละปัจจัยที่องค์กรจะต้องสนับสนุน ปรับปรุง และให้ความสำคัญมากขึ้น เพื่อทำให้การสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์เกิดขึ้นและยั่งยืนในองค์กร

2. ควรมีการศึกษาเรื่องการวิเคราะห์ช่องว่าทางศักยภาพ (Gab Analysis) ในบริบทขององค์กรในไทย เพื่อนำมาวิเคราะห์ช่องว่างในมุมมองด้านต่าง ๆ ว่ามีผลต่อการสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์อย่างไร

บรรณานุกรม

กรินธัญญวิกรม และ ธีระ กุลสวัสดิ์. (2564). **การจัดการความมั่นคงทางเทคโนโลยีสารสนเทศกรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย**. สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยบูรพา.

จิราพัชร์ พันธุ์ถาวรชัย. (2561). **แนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์**. สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยศรีปทุม.

ชฎาภรณ์ สิงห์แก้ว. (2564). **บทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม.** วารสารวิชาการมหาวิทยาลัยการจัดการและเทคโนโลยีอีสเทิร์น ปีที่ 18 ฉบับที่ 1 มกราคม – มิถุนายน 2564

ชนินทร เฉลิมทรัพย์. (2560-2561). **แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ.** งานวิจัยของหลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 60. วิทยาลัยป้องกันราชอาณาจักร

ชาย นครชัย. (2561). **การส่งเสริมความเข้มแข็งของวัฒนธรรมไทย : ศึกษามุมมองของเยาวชนไทยต่อการรุกคืบของวัฒนธรรมต่างชาติ.** งานวิจัยของหลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 60. วิทยาลัยป้องกันราชอาณาจักร

ณัทรัฏฐ์ มณีรัสยากร. (2559). **การพัฒนานโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO27001ขององค์กรกรณีศึกษา บจก. เซ็กโก้ เอ็นจิเนียริ่ง แอนด์ คอนสตรัคชั่น.** สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยเทคโนโลยีมหานคร

ติตสุภา ฤทธิผสิน. (2564). **กลยุทธ์การคืนสภาพทางไซเบอร์ : แนวทางสำคัญในการดำเนินงานขององค์กรในยุคดิจิทัล ของ กสทช.**

เบญญาภา ปัญญา. (2562). **การควบคุมตนเองของเจ้าหน้าที่ตำรวจสายตรวจในสังกัดกองบังคับการตำรวจนครบาล 2**. วารสารวิจัยวิชาการมหาวิทยาลัยราชภัฏสวนสุนันทา ปีที่ 3 ฉบับที่ 2 (พฤษภาคม-สิงหาคม 2563)

ปวีณ์กร คลังข้อง. (2559). **วัฒนธรรมวิจัยของครูในจังหวัดปัตตานี.** วิทยานิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยสงขลานครินทร์

วสุนธรา รตโนภาส และคณะ. (2558). **ความสัมพันธ์ของวัฒนธรรมองค์กรกับระดับความสุขของบุคลากรในสถานประกอบการอุตสาหกรรมสิ่งทอและเครื่องนุ่งห่ม อำเภอแม่สอด จังหวัดตาก.** งานวิจัย. มหาวิทยาลัยราชภัฏกำแพงเพชร

วิลาส วิถีไพร. (2561). **การพัฒนากรอบการรักษาความมั่นคงปอลดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง.** สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยศรีปทุม

ศิวลีย์ สิริดรจน์บริรักษ์. (2558). **การพัฒนามาตรฐานการรักษาความมั่นคงไซเบอร์ (Cyber security) ของกระทรวงกลาโหม**.วารสารสถาบันวิชาการป้องกันประเทศ.ปีที่ 6 (ฉบับที่ 3).

เศรษฐพงศ์ มะลิสุวรรณ. (2558). **แนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Strategy) ของ กสทช.**

สมคิด สกุลสถาปัตย์. (2563). **กลยุทธ์การสร้างวัฒนธรรมคุณภาพในการบริหารจัดการสถานศึกษาขั้นพื้นฐาน**. วารสาร “ศึกษาศาสตร์ มมร” คณะศึกษาศาสตร์ มหาวิทยาลัยมหามกุฏราชวิทยาลัย ปีที่ 8 ฉบับที่ 1 (มกราคม – มิถุนายน 2563)

สุธาเทพ รุณเรศ. (2561). **ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร**. สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยธรรมศาสตร์.

สุพิตรา ศรีบุรินทร์ และ ทัชชกร แสงทองดี. (2564). **การตระหนักรู้ในการป้องกันตนเองบนโลกไซเบอร์ของประชาชนในเขตเทศบาลตำบลอ้อมใหญ่**. วารสารอาชญากรรมและความปลอดภัย ปีที่ 3 ฉบับที่ 1 (มกราคม-มิถุนายน 2564)

สุรพงศ์ ทรัพยาคม และอรรถพล ป้อมสถิตย์. (2563). **การวิเคราะห์การรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**. เอกสารสืบเนื่องจากการประชุมวิชาการระดับชาติมหาวิทยาลัยรังสิต ประจำปี 2563 เผยแพร่ออนไลน์ : ลิขสิทธิ์ © 2559-2563 มหาวิทยาลัยรังสิต

หนึ่งฤทัย กอสง่าลักษณ์. (2557). **การพัฒนาเครื่องมือการวิเคราะห์เชิงจินตภาพในการวิจัยด้านความปลอดภัยทางไซเบอร์**. สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยากรุงเทพ.

ปริญญ์ เสรีพงศ์. (2557). **เรียนรู้มาตรฐาน ISO 27001 : 2013 การจัดการความมั่นคงปลอดภัยของสารสนเทศแบบง่ายๆ** สืบค้นเมื่อวันที่ 10 ธันวาคม 2564 จากเว็บไซต์ www.club27001.com/2013

โครงการส่งเสริมการพัฒนาทักษะและศักยภาพกำลังคนด้านความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยธรรมศาสตร์ **หลักสูตร “Cyber Security for Cloud and Network”.** สืบค้นเมื่อวันที่ 10 ธันวาคม 2564 จากเว็บไซต์ https://sites.google.com/storemesh.com/depacybersecurity/course-materials

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (2564). **ระบบมาตรฐานด้านความปลอดภัยสารสนเทศ ISO 27001 หรือ ISO/IEC 27001:2013**. สืบค้นเมื่อวันที่ 10 ธันวาคม 2564 จากเว็บไซต์ www.dga.or.th/document-sharing/article/36059.

บริษัทโทรคมนาคมแห่งชาติ จำกัด (มหาชน). (2564). **ทำความรู้จักกับ NIST Cybersecurity Framework.** สืบค้นเมื่อวันที่ 10 ธันวาคม 2564 จากเว็บไซต์ www.cyfence.com/article/nist-cybersecurity-framework.

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแหงชาติ (สวทช. หรือ NSTDA). (2564). **แนวคิดเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)** . สืบค้นเมื่อวันที่ 10 ธันวาคม 2564 จากเว็บไซต์ www.nstda.or.th

European Union Agency for Network and Information Security. (2017). **Cyber Security Culture in Organisations**. Retrieved July 24, 2018 from https:// www.enisa.europa.eu.

Gioulekas Fotios, Stamatiadis Evangelos, Tzikas Athanasios, ... Gounaris Konstantinos,et al. **(2565). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures**. Healthcare 2022, 10, 327. from https://doi.org/10.3390/healthcare10020327

Kerstan S. Cole, Susan M. Stevens-Adams, & Caren A. Wenner. (2013). **A Literature Review of Safety Culture**. Retrieved July 24, 2018 from https://prod.sandia.gov/techlib-noauth/access-control.cgi/2013/132754.pdf

Kabanda Gabriel. (2561). **A Cybersecurity Culture Framework and Its Impact on Zimbabwean Organizations**. Asian Journal of Management, Engineering & Computer Sciences (AJMECS)

Miranda, Michael. (2561). **Enhancing Cybersecurity Awareness Training: A Comprehensive Phishing Exercise Approach**. International Management Review Vol. 14 No. 2

Uchendu Betsy, Nurse R.C., Bada Maria & Furnell Steven. (2564). **Developing a cyber security culture: Current practices and future needs**. Computers & Security Journal

Wajeb Gharibi and Maha Shaabi. (2555). **Cyber Threats in Social Networking Websites**. College of Computer Science & Information SystemsJazan University, Kingdom of Saudi Arabia

ภาคผนวก ก

แบบสอบถาม

แบบสอบถามเชิงคุณภาพ

เรื่อง การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร
สำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

แบบสอบถามเชิงคุณภาพ

เรื่อง การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร สำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

เพื่อใช้สำหรับการศึกษา

ในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

<u>คำชี้แจง</u>

แบบสอบถามนี้ได้จัดทำขึ้นเพื่อสอบถามความคิดเห็นของท่านเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในองค์กร ซึ่งเป็นส่วนหนึ่งของการวิจัยของมหาวิทยาลัยศรีปทุม โดยมีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ส่งผลต่อการสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

ทางมหาวิทยาลัยศรีปทุม ใคร่ขอความร่วมมือท่านให้ข้อมูลหรือแสดงความคิดเห็นที่ตรงกับความเป็นจริงมากที่สุด ข้อมูลที่ได้จะนำไปใช้ประกอบการศึกษาทางด้านวิชาการเท่านั้น ผู้วิจัยขอรับรองว่าการตอบแบบสอบถามนี้จะไม่มีผลกระทบหรือก่อให้เกิดความเสียหายต่อตัวท่านแต่ประการใดและขอขอบพระคุณท่านในการให้ความกรุณาตอบแบบสอบถามทุกข้อ

ข้อคำถามแบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 ข้อมูลส่วนบุคคลหรือหน่วยงานของผู้ตอบแบบสอบถาม

ส่วนที่ 2 ข้อคำถามเกี่ยวกับความคิดเห็นเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในองค์กร

ส่วนที่ 3 ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

ส่วนที่ 1 ข้อมูลผู้ตอบแบบสอบถาม

ชื่อผู้ให้สัมภาษณ์ .....

ตำแหน่ง .....

สถานที่ทำงาน .....

ประสบการณ์ในการทำงาน .....

ผู้วิจัย : นางสาวฐิติมา ภู่ห้อย
นักศึกษาหลักสูตรวิทยาศาตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
E-mail : thitimaphuhoy@gmail.com โทรศัพท์ โทรศัพท์ : 086-361-9211

นิยามศัพท์เฉพาะ

วัฒนธรรมความมั่นคงปลอดภัยไซเบอร์	หมายถึง คุณลักษณะ ทัศนคติ ของบุคคลกรและองค์กร เพื่อสนับสนุน เสริมสร้าง รวมทั้งทำให้เกิดความยั่งยืนด้านความมั่นคงปลอดภัยไซเบอร์
การเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Transformation)	หมายถึง กระบวนการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ เป็นการเปลี่ยนทัศนคติและสร้างวัฒนธรรม ทางความมั่นคงปลอดภัยไซเบอร์ที่หยั่งรากลึกในระดับบุคคลและองค์กรให้เกิดภูมิคุ้มกัน และมีจริยธรรมทางความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้เพื่อสร้างความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ อีกทั้งยังทำให้บุคคลและองค์กรมีขีดความสามารถด้านไซเบอร์ ในอันที่จะป้องกันต่อต้าน ตรวจจับ และตอบสนองต่อการบุกรุก การจารกรรม หรือการหลอกลวง ที่จะทำให้เกิดความเสียหายได้
ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)	หมายถึง ภาวะพ้นจากภัยคุกคามที่มีต่อเครือข่าย ระบบคอมพิวเตอร์ โปรแกรม และข้อมูล เพื่อรักษาไว้ซึ่งลักษณะสำคัญ 3 ประการ คือ ความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน ภาวะดังกล่าวจะเกิดขึ้นได้ ต้องอาศัยบุคลากร กระบวนการทำงาน และเครื่องมือที่เหมาะสม
ไซเบอร์ (Cyber)	หมายถึง คำที่ใช้เติมหน้าคำอื่นเพื่อแสดงความเกี่ยวข้องกับเครือข่ายคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือ อินเทอร์เน็ต หรือความเป็นจริงเสมือน (Virtual Reality) เช่น ไซเบอร์สเปซ (Cyberspace) หมายถึง สภาพแวดล้อมสมมติในเครือข่ายอินเทอร์เน็ต

ส่วนที่ 2 ข้อคำถามเกี่ยวกับความคิดเห็นเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในองค์กร

ข้อที่ 1 ในมุมมองของท่าน ในปัจจุบันปัญหาและอุปสรรคด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กรเป็นอย่างไร

.....

.....

.....

.....

.....

ข้อที่ 2 ในมุมมองของท่าน ความพร้อมด้านความมั่นคงปลอดภัยในองค์กรเป็นอย่างไร

.....

.....

.....

.....

.....

ข้อที่ 3 ในมุมมองของท่าน คิดว่ามีปัจจัยอะไรที่จะทำให้การรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กรประสบความสำเร็จ

.....

.....

.....

.....

.....

ข้อที่ 4 จากคำตอบข้อที่ 3 ท่านคิดว่าควรมีการส่งเสริมหรือปรับปรุงในแต่ละปัจจัยอย่างไร

.....

.....

.....

.....

.....

ข้อที่ 5 ท่านคิดว่าการสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ มีความสำคัญอย่างไร

.....

.....

.....

.....

.....

ส่วนที่ 3 ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

ท่านมีความคิดเห็นหรือข้อเสนอแนะอย่างไร เกี่ยวกับการสร้างกรอบหรือองค์ประกอบการสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กร

.....

.....

.....

.....

.....

ขอขอบพระคุณที่ท่านได้กรุณาเสียสละเวลาในการตอบแบบสอบถาม

รายนามผู้บริหารและผู้เชี่ยวชาญด้านระบบเครือข่ายของสารสนเทศกลางของหน่วยงาน
กรุงเทพมหานคร และของสำนักการวางผังและพัฒนาเมือง

รายนามผู้บริหารและผู้เชี่ยวชาญด้านระบบเครือข่ายของสารสนเทศกลางของหน่วยงาน
กรุงเทพมหานคร และของสำนักการวางผังและพัฒนาเมือง

หน่วยงาน สำนักยุทธศาสตร์และประเมินผล

1. นางสาวอรพรรณ ศรีเกตุ ผู้อำนวยการเฉพาะด้าน
(วิชาการคอมพิวเตอร์)
กองพัฒนาระบบงานคอมพิวเตอร์
ประสบการณ์ในการทำงาน - ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ 18 ปี
- ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ (หัวหน้ากลุ่มงาน) 6 ปี
- ดำรงตำแหน่งอำนวยการต้น 2 ปี

2. นายธนวัฒน์ จิระพันธ์พงศ์ หัวหน้าฝ่ายระบบเครื่องและเครือข่าย
กองควบคุมระบบคอมพิวเตอร์
ประสบการณ์ในการทำงาน - ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ 20 ปี
- ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ (หัวหน้ากลุ่มงาน) 2 ปี

3. นายสารสิน อิ่มโอษฐ์ หัวหน้าฝ่ายแผนงาน
กองพัฒนาระบบงานคอมพิวเตอร์
ประสบการณ์ในการทำงาน - ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ 18 ปี
- ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ (หัวหน้ากลุ่มงาน) 4 ปี

4. นายเปรมชาย จงเจริญ หัวหน้าฝ่ายฐานข้อมูล
กองควบคุมระบบคอมพิวเตอร์
ประสบการณ์ในการทำงาน - ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ 16 ปี
- ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ (หัวหน้ากลุ่มงาน) 2 ปี

5. นางอภิรดี ศรีวงษา นักวิชาการคอมพิวเตอร์ชำนาญการ
ฝ่ายแผนงาน กองพัฒนาระบบงานคอมพิวเตอร์
ประสบการณ์ในการทำงาน ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ 24 ปี

6. นางพิมพา จันทอง นักวิชาการคอมพิวเตอร์ชำนาญการ
ฝ่ายโปรแกรมระบบ กองควบคุมระบบคอมพิวเตอร์
ประสบการณ์ในการทำงาน ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ 24 ปี

7. นายศุภชัย วงศ์วิวัฒน์ นักวิชาการคอมพิวเตอร์ชำนาญการ
ฝ่ายระบบเครื่องและเครือข่าย
กองควบคุมระบบคอมพิวเตอร์
ประสบการณ์ในการทำงาน ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ 22 ปี

8. นายพนมไพร ไชยศล นักวิชาการคอมพิวเตอร์ชำนาญการ
ฝ่ายระบบเครื่องและเครือข่าย
กองควบคุมระบบคอมพิวเตอร์
ประสบการณ์ในการทำงาน ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ 22 ปี

9. นายสิทธิพร รัตนจันทร์ นักวิชาการคอมพิวเตอร์ชำนาญการ
ฝ่ายโปรแกรมระบบ กองควบคุมระบบคอมพิวเตอร์
ประสบการณ์ในการทำงาน ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ 10 ปี

10. นายสุทธิพงษ์ ตั้งวงศ์งาม นักวิชาการคอมพิวเตอร์ชำนาญการ
ฝ่ายระบบเครื่องและเครือข่าย
กองควบคุมระบบคอมพิวเตอร์
ประสบการณ์ในการทำงาน ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ 10 ปี

11. ว่าที่ร้อยตรี อรรณพ สัมพันธวรบุตร นักวิชาการคอมพิวเตอร์ชำนาญการ
ฝ่ายแผนงาน กองพัฒนาระบบงานคอมพิวเตอร์
ประสบการณ์ในการทำงาน ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ 4 ปี 10 เดือน

หน่วยงาน สำนักการวางผังและพัฒนาเมือง

1. นายสุดใจ ยี่สุ่นแสง ตำแหน่งผู้อำนวยการสำนักงานภูมิสารสนเทศ
สำนักงานภูมิสารสนเทศ
ประสบการณ์ในการทำงาน ดำรงตำแหน่งอำนวยการระดับสูง 3 ปี

2. นายโชคทวี องค์เจริญสุข หัวหน้ากลุ่มงานสารสนเทศ
สำนักงานภูมิสารสนเทศ
ประสบการณ์ในการทำงาน - ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ 20 ปี
- ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ (หัวหน้ากลุ่มงาน) 3 ปี

3. นางนงลักษณ์ ทรรพนันท์ นักวิชาการคอมพิวเตอร์ชำนาญการ
กลุ่มงานข้อมูลเมือง ศูนย์เทคโนโลยีข้อมูลเมือง
สำนักงานภูมิสารสนเทศ
ประสบการณ์ในการทำงาน ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ 29 ปี

4. นางธิรดา คงนวล นักวิชาการคอมพิวเตอร์ปฏิบัติการ
กลุ่มงานสารสนเทศ ศูนย์เทคโนโลยีข้อมูลเมือง
สำนักงานภูมิสารสนเทศ
ประสบการณ์ในการทำงาน ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ 12 ปี

แบบสอบถามเชิงปริมาณ

เรื่อง การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร
สำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

เลขที่แบบสอบถาม.....

แบบสอบถามการวิจัย
เรื่อง “การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร
สำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์”

<u>คำชี้แจง</u>

แบบสอบถามนี้เป็นส่วนหนึ่งของการวิจัยของทางมหาวิทยาลัยศรีปทุม โดยมีวัตถุประสงค์เพื่อศึกษาพฤติกรรมและความพร้อมของบุคลากรที่มีต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ทางมหาวิทยาลัยศรีปทุม ใคร่ขอความร่วมมือและขอขอบพระคุณท่านในการให้ความกรุณาตอบแบบสอบถามทุกข้อ โดยข้อมูลที่ได้นี้จะได้นำไปใช้ประกอบการศึกษาเพื่อประโยชน์ทางด้านวิชาการเท่านั้น ขอรับรองว่าการตอบแบบสอบถามนี้จะไม่มีผลกระทบหรือก่อให้เกิดความเสียหายต่อตัวท่านแต่ประการใด

แบบสำรวจแบ่งออกเป็น 3 ส่วนคือ

ส่วนที่ 1 : ข้อมูลส่วนบุคคลหรือหน่วยงานของผู้ตอบแบบสอบถาม

ส่วนที่ 2 : ข้อคำถามเกี่ยวกับความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ส่วนที่ 3: ข้อคำถามเกี่ยวกับพฤติกรรมเสี่ยงต่อภัยคุกคามต่อระบบเครือข่ายของหน่วยงาน

โปรดพิจารณาข้อคำถามต่อไปนี้แล้วทำเครื่องหมาย ✓ ลงในช่องที่ตรงกับความจริงหรือความคิดเห็นหรือความรู้สึกของท่านมากที่สุดเพียงช่องเดียวแบ่งระดับคำตอบเป็น 5 ระดับ ดังนี้

5	หมายถึง	เป็นจริงหรือเห็นด้วยมากที่สุด
4	หมายถึง	เป็นจริงหรือเห็นด้วยมาก
3	หมายถึง	เป็นจริงหรือเห็นด้วยปานกลาง
2	หมายถึง	เป็นจริงหรือเห็นด้วยน้อย
1	หมายถึง	ไม่เป็นจริงหรือเห็นด้วยน้อยที่สุด

นางสาวฐิติมา ภู่ห้อย E-mail:Thitimaphuhoy@gmail.com โทรศัพท์: 063-156-1466
นักศึกษาหลักสูตรศึกษาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

นิยามศัพท์

วัฒนธรรมความมั่นคงปลอดภัยไซเบอร์	หมายถึง คุณลักษณะ ทัศนคติ ของบุคคลกรและองค์กร เพื่อสนับสนุน เสริมสร้าง รวมทั้งทำให้เกิดความยั่งยืนด้านความมั่นคงปลอดภัยไซเบอร์
การเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Transformation)	หมายถึง กระบวนการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ เป็นการเปลี่ยนทัศนคติและสร้างวัฒนธรรม ทางความมั่นคงปลอดภัยไซเบอร์ที่หยั่งรากลึกในระดับบุคคลและองค์กรให้เกิดภูมิคุ้มกัน และมีจริยธรรมทางความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้เพื่อสร้างความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ อีกทั้งยังทำให้บุคคลและองค์กรมีขีดความสามารถด้านไซเบอร์ ในอันที่จะป้องกันต่อต้าน ตรวจจับ และตอบสนองต่อการบุกรุก การจารกรรม หรือการหลอกลวง ที่จะทำให้เกิดความเสียหายได้
ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)	หมายถึง ภาวะพ้นจากภัยคุกคามที่มีต่อเครือข่าย ระบบคอมพิวเตอร์ โปรแกรม และข้อมูล เพื่อรักษาไว้ซึ่งลักษณะสำคัญ 3 ประการ คือ ความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน ภาวะดังกล่าวจะเกิดขึ้นได้ ต้องอาศัยบุคลากร กระบวนการทำงาน และเครื่องมือที่เหมาะสม
ไซเบอร์ (Cyber)	หมายถึง คำที่ใช้เติมหน้าคำอื่นเพื่อแสดงความเกี่ยวข้องกับเครือข่ายคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือ อินเทอร์เน็ต หรือความเป็นจริงเสมือน (Virtual Reality) เช่น ไซเบอร์สเปซ (Cyberspace) หมายถึง สภาพแวดล้อมสมมติในเครือข่ายอินเทอร์เน็ต

ส่วนที่ 1: ข้อมูลส่วนบุคคลหรือหน่วยงานของผู้ตอบแบบสอบถาม

คำชี้แจง โปรดทำเครื่องหมาย ☑ ลงในช่องที่ตรงกับข้อมูลส่วนบุคคลของท่าน

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ ต่ำกว่า 30 ปี ☐ 30-40 ปี

☐ 41-50 ปี ☐ 51-60 ปี

3. ระดับการศึกษาสูงสุด

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี

☐ ปริญญาโท ☐ ปริญญาเอก

4. สายงานที่ปฏิบัติ

☐ ด้านบริหาร ☐ ด้านปฏิบัติการ

☐ ด้านธุรการ ☐ ด้านอื่น ๆ

5. ท่านได้ปฏิบัติงานในหน่วยงานแห่งนี้มานานเท่าใด

☐ ไม่เกิน 5 ปี ☐ 6 – 10 ปี

☐ 11 – 15 ปี ☐ 16 ปีขึ้นไป

6. ท่านได้ใช้เวลาโดยเฉลี่ยอยู่กับคอมพิวเตอร์นานเท่าใด ในแต่ละวันของเวลาทำงาน

☐ น้อยกว่า 1 ชั่วโมงต่อวัน ☐ 1 - 3 ชั่วโมงต่อวัน

☐ 4 – 6 ชั่วโมงต่อวัน ☐ มากกว่า 6 ชั่วโมงต่อวัน

ส่วนที่ 2: ข้อคำถามเกี่ยวกับความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงในช่องที่**ตรงกับความคิดเห็นหรือความรู้สึกของท่านมากที่สุด** เพียงช่องเดียว

(5 = เห็นด้วยมากที่สุด, 4 = เห็นด้วยมาก, 3 = เห็นด้วยปานกลาง, 2 = เห็นด้วยน้อย, 1 = เห็นด้วยน้อยที่สุด)

ความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยไซเบอร์	ระดับความคิดเห็น				
	5	4	3	2	1
1. ท่านคิดว่าการเข้าเว็บไซต์ https มีความปลอดภัยกว่า http					
2. ท่านคิดว่าการเปิดเผยระบุตัวตนบนเครือข่ายสังคมออนไลน์สาธารณะที่มีผู้ใช้ทั่วไปมีความปลอดภัย					
3. ท่านคิดว่าการให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะไม่มีความเสี่ยง					
4. ท่านคิดว่าการเข้าใช้งานเครือข่ายไร้สายสาธารณะมีความเสี่ยงต่อการทำธุรกรรมออนไลน์					
5. ท่านคิดว่าการติดตามข่าวสารรูปแบบการโจมตีทางไซเบอร์ช่วยป้องกันความเสียหายที่จะเกิดขึ้นได้					
6. ท่านคิดว่าการสำรองข้อมูลและตั้งรหัสการเข้าใช้งานทำให้อุปกรณ์ของท่านมีความปลอดภัยมากยิ่งขึ้น					

ส่วนที่ 3: ข้อคำถามเกี่ยวกับพฤติกรรมเสี่ยงต่อภัยคุกคามต่อระบบเครือข่ายของหน่วยงาน

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงในช่องที่**ตรงกับความคิดเห็นหรือความรู้สึกของท่านมากที่สุด** เพียงช่องเดียว

(5 = เห็นด้วยมากที่สุด, 4 = เห็นด้วยมาก, 3 = เห็นด้วยปานกลาง, 2 = เห็นด้วยน้อย, 1 = เห็นด้วยน้อยที่สุด)

ข้อ	พฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในหน่วยงาน	ระดับความความคิดเห็น				
		5	4	3	2	1
ด้านพฤติกรรมการใช้อินเทอร์เน็ต						
1	การใช้อีเมลตนเองในการสมัครบัญชีออนไลน์					
2	การตั้งค่าบัญชีให้เป็นส่วนตัว					
3	การกรอกข้อมูลส่วนตัวตามอีเมลที่ส่งมา					

ข้อ	พฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในหน่วยงาน	ระดับความความคิดเห็น				
		5	4	3	2	1
4	การดาวน์โหลดไฟล์โดยไม่ทราบแหล่งที่มาออนไลน์					
5	การเข้าเว็บไซต์ที่ไม่เหมาะสม					
ด้านพฤติกรรมการใช้งานสื่อสังคม						
1	การเผยแพร่ข้อความ รูปภาพ วิดิทัศน์ ลงในสื่อสาธารณะ					
2	อนุญาตให้บุคคลที่ไม่รู้จักเข้าถึงการใช้งานบน Social Media ของตนเอง					
3	ไม่จำกัดการเข้าถึงข้อมูลส่วนตัวใจบัญชี Social Media					
ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์						
1	การเข้าถึงสื่อออนไลน์ที่ไม่รู้จักมาก่อน					
2	การเข้าถึงสื่อที่มีโฆษณาเชิญชวนไปยังเว็บไซต์อื่น					
3	การเข้าถึงสื่อออนไลน์ที่ไม่ได้รับการคัดกรอง					
4	การเข้าสื่อออนไลน์ที่ให้เปิดเผยข้อมูลส่วนตัวมากเกินไป					
ด้านพฤติกรรมการใช้งานผ่านโปรแกรม						
1	การใช้งานผ่านโปรแกรมที่ไม่มีลิขสิทธิ์					
2	การโหลดโปรแกรมที่ไม่มีลิขสิทธิ์จากแหล่งต่าง ๆ					
3	การติดตั้งโปรแกรมต่าง ๆ จากบุคคลอื่น					
4	การติดตั้งโปรแกรมโดยไม่ศึกษารายละเอียด					
ด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต						
1	มีโปรแกรมป้องกัน Spyware					
2	การเปิดการใช้งานโปรแกรม Firewall					
3	มีการสำรอง (Backup) ข้อมูลเป็นประจำ					
4	มีโปรแกรมสำหรับลบไฟล์แบบถาวร (Files Shredder)					

ส่วนที่ 4: ความคิดเห็นและข้อเสนอแนะอื่น ๆ

.....

.....

.....

ขอขอบพระคุณที่ท่านได้กรุณาเสียสละเวลาในการตอบแบบสอบถาม

ภาคผนวก ข

แบบตรวจสอบคุณภาพเครื่องมือการวิจัย

แบบสอบถามการวิจัย
แบบตรวจสอบคุณภาพเครื่องมืองานวิจัย

เรื่อง "การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์"

คำชี้แจง : แบบสอบถามนี้เป็นส่วนหนึ่งของการวิจัยของทางมหาวิทยาลัยศรีปทุม โดยมีวัตถุประสงค์เพื่อศึกษาพฤติกรรมและความพร้อมของบุคลากรที่มีต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ทางมหาวิทยาลัยศรีปทุม ใคร่ขอความร่วมมือและขอขอบพระคุณท่านในการให้ความกรุณาตอบแบบสอบถามทุกข้อ โดยข้อมูลที่ได้นี้จะได้นำไปใช้ประกอบการศึกษาเพื่อประโยชน์ทางด้านวิชาการเท่านั้น ขอรับรองว่าการตอบแบบสอบถามนี้จะไม่มีผลกระทบหรือก่อให้เกิดความเสียหายต่อตัวท่านแต่ประการใด

แบบสำรวจแบ่งออกเป็น 3 ส่วนคือ

ส่วนที่ 1: ข้อมูลส่วนบุคคลหรือหน่วยงานของผู้ตอบแบบสอบถาม

ส่วนที่ 2: ข้อคำถามเกี่ยวกับความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ส่วนที่ 3: ข้อคำถามเกี่ยวกับพฤติกรรมเสี่ยงต่อภัยคุกคามต่อระบบเครือข่ายของหน่วยงาน

<u>คำชี้แจง</u> : ให้ท่านพิจารณาว่า ข้อคำถามแต่ละข้อต่อไปนี้ มีความสอดคล้องกับวัตถุประสงค์ในการวัดหรือไม่ โดยให้ท่านทำเครื่องหมาย / ลงในช่องว่างหลังข้อคำถามแต่ละข้อ โดยมีเกณฑ์ในการพิจารณา ดังนี้

1 หมายถึง ท่านเห็นว่าข้อความนั้นมีความสอดคล้องกับวัตถุประสงค์

0 หมายถึง ท่านไม่แน่ใจว่าข้อคำถามนั้นมีความสอดคล้องกับวัตถุประสงค์หรือไม่

-1 หมายถึง ท่านเห็นว่าข้อความนั้นไม่สอดคล้องกับวัตถุประสงค์

ลงนามชื่อผู้เชี่ยวชาญ .....

(.....)

นิยามศัพท์

วัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ หมายถึง คุณลักษณะ ทัศนคติ ของบุคคลกรและองค์กรเพื่อสนับสนุน เสริมสร้าง รวมทั้งทำให้เกิดความยั่งยืนด้านความมั่นคงปลอดภัยไซเบอร์

การเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ หมายถึง กระบวนการสร้างความตระหนักรู้ด้านความมั่นคง ปลอดภัยไซเบอร์ เป็นการเปลี่ยนทัศนคติและสร้างวัฒนธรรมทางความมั่นคงปลอดภัยไซเบอร์ที่หยั่งรากลึกในระดับบุคคลและองค์กรให้เกิดภูมิคุ้มกัน และมีจริยธรรมทางความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้เพื่อสร้างความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ อีกทั้งยังทำให้บุคคลและองค์กรมีขีดความสามารถด้านไซเบอร์ที่จะป้องกันต่อต้านตรวจจับ และตอบสนองต่อการบุกรุกการจารกรรม หรือการหลอกลวง ที่จะทำให้เกิดความเสียหายได้

ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) หมายถึง ภาวะพ้นจากภัยคุกคามที่มีต่อเครือข่ายระบบคอมพิวเตอร์ โปรแกรม และข้อมูล เพื่อรักษาไว้ซึ่งลักษณะสำคัญ 3 ประการ คือ ความลับ ความถูกต้อง ครบถ้วน และความพร้อมใช้งาน ภาวะดังกล่าวจะเกิดขึ้นได้ต้องอาศัยบุคลากร กระบวนการทำงาน และเครื่องมือที่เหมาะสม

ไซเบอร์ (Cyber) หมายถึง คำที่ใช้เติมหน้าคำอื่นเพื่อแสดงความเกี่ยวข้องกับเครือข่ายคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรืออินเทอร์เน็ต หรือความเป็นจริงเสมือน เช่น ไซเบอร์สเปซ (Cyberspace) หมายถึงสภาพแวดล้อม สมมติในเครือข่ายอินเทอร์เน็ต

ส่วนที่ 2 ข้อคำถามเกี่ยวกับความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			

ข้อ	ความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยไซเบอร์								
1	ท่านคิดว่าการเข้าเว็บไซต์ https มีความปลอดภัยกว่า http	1	1	1	1	-1	0.6	ใช้ได้	ควรมีคำอธิบายก่อนหน้าถึงความแตกต่างระหว่าง https และ http
2	ท่านคิดว่าการเปิดเผยระบุตัวตนบนเครือข่ายสังคมออนไลน์สาธารณะที่มีผู้ใช้ทั่วไปมีความปลอดภัย	1	1	1	1	1	1	ใช้ได้	ควรมีความระวังเรื่อง “ตัวเลือกตอบ” ของข้อคำถามข้อนี้
3	ท่านคิดว่าการให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะไม่มีความเสี่ยง	1	1	1	0	1	0.8	ใช้ได้	ควรมีความระวังเรื่อง “ตัวเลือกตอบ” ของข้อคำถามข้อนี้

ส่วนที่ 2 (ต่อ)ข้อคำถามเกี่ยวกับความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			

ข้อ	ความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยไซเบอร์								
4	ท่านคิดว่าการเข้าใช้งานเครือข่ายไร้สายสาธารณะมีความเสี่ยงต่อการทำธุรกรรมออนไลน์	1	1	0	1	1	0.8	ใช้ได้	ควรมีความระวังเรื่อง “ตัวเลือกตอบ” ของข้อคำถามข้อนี้
5	ท่านคิดว่าการติดตามข่าวสารรูปแบบการโจมตีทางไซเบอร์ช่วยป้องกันความเสียหายที่จะเกิดขึ้นได้	1	1	0	0	1	0.6	ใช้ได้	ควรมีความระวังเรื่อง “ตัวเลือกตอบ” ของข้อคำถามข้อนี้
6	ท่านคิดว่าการสำรองข้อมูลและตั้งรหัสการเข้าใช้งานทำให้อุปกรณ์ของท่านมีความปลอดภัยมากยิ่งขึ้น	1	1	1	1	1	1	ใช้ได้	ควรมีความระวังเรื่อง “ตัวเลือกตอบ” ของข้อคำถามข้อนี้

ส่วนที่ 3 ข้อคำถามเกี่ยวกับพฤติกรรมเสี่ยงต่อภัยคุกคามต่อระบบเครือข่ายของหน่วยงาน

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			

พฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในหน่วยงาน									
<u>ด้านพฤติกรรมการใช้อินเทอร์เน็ต</u>									
7	การใช้อีเมลตนเองในการสมัครบัญชีออนไลน์	1	0	1	1	1	0.8	ใช้ได้	ควรจะให้มีการตั้งหัวข้อคำถามที่เป็นไปในทิศทางเดียวกัน (ให้เป็นทิศทางบวกเดียวกันหรือไม่ก็ ให้เป็นทิศทางลบเดียวกัน)
8	การตั้งค่าบัญชีให้เป็นส่วนตัว	1	1	1	0	1	0.8	ใช้ได้	
9	การกรอกข้อมูลส่วนตัวตามอีเมลที่ส่งมา	1	0	1	1	1	0.8	ใช้ได้	
10	การดาวน์โหลดไฟล์โดยไม่ทราบแหล่งที่มาออนไลน์	1	1	0	1	1	0.8	ใช้ได้	
11	การเข้าเว็บไซต์ที่ไม่เหมาะสม	1	1	0	1	1	0.8	ใช้ได้	
<u>ด้านพฤติกรรมการใช้งานสื่อสังคม</u>									
12	การเผยแพร่ข้อความ รูปภาพ วิดิทัศน์ ลงในสื่อสาธารณะ	1	1	1	1	1	1	ใช้ได้	

ส่วนที่ 3 (ต่อ) ข้อคำถามเกี่ยวกับพฤติกรรมเสี่ยงต่อภัยคุกคามต่อระบบเครือข่ายของหน่วยงาน

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			

พฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในหน่วยงาน									
13	อนุญาตให้บุคคลที่ไม่รู้จักเข้าถึงการใช้งานบน Social Media ของตนเอง	1	1	1	1	1	1	ใช้ได้	
14	ไม่จำกัดการเข้าถึงข้อมูลส่วนตัวใจบัญชี Social Media	1	1	1	1	1	1	ใช้ได้	
<u>ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์</u>									
15	การเข้าถึงสื่อออนไลน์ที่ไม่รู้จักมาก่อน	1	1	1	1	1	1	ใช้ได้	
16	การเข้าถึงสื่อที่มีโฆษณาเชิญชวนไปยังเว็บไซต์อื่น	1	1	1	1	1	1	ใช้ได้	
17	การเข้าถึงสื่อออนไลน์ที่ไม่ได้รับการคัดกรอง	1	0	1	1	1	0.8	ใช้ได้	
18	การเข้าสื่อออนไลน์ที่ให้เปิดเผยข้อมูลส่วนตัวมากเกินไป	1	1	1	1	1	1	ใช้ได้	
<u>ด้านพฤติกรรมการใช้งานผ่านโปรแกรม</u>									
19	การใช้งานผ่านโปรแกรมที่ไม่มีลิขสิทธิ์	1	1	0	1	1	0.8	ใช้ได้	
20	การโหลดโปรแกรมที่ไม่มีลิขสิทธิ์จากแหล่งต่าง ๆ	1	1	0	1	1	0.8	ใช้ได้	
21	การติดตั้งโปรแกรมต่าง ๆ จากบุคคลอื่น	1	1	1	1	1	1	ใช้ได้	

ส่วนที่ 3 (ต่อ) ข้อคำถามเกี่ยวกับพฤติกรรมเสี่ยงต่อภัยคุกคามต่อระบบเครือข่ายของหน่วยงาน

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			

พฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในหน่วยงาน									
22	การติดตั้งโปรแกรมโดยไม่ศึกษารายละเอียด	1	1	0	1	1	0.8	ใช้ได้	
<u>ด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต</u>									
23	มีโปรแกรมป้องกัน Spyware	1	1	0	1	1	0.8	ใช้ได้	
24	การเปิดการใช้งานโปรแกรม Firewall	1	1	0	1	1	0.8	ใช้ได้	
25	มีการสำรอง (Backup) ข้อมูลเป็นประจำ	1	1	0	1	1	0.8	ใช้ได้	
26	มีโปรแกรมสำหรับลบไฟล์แบบถาวร (Files Shredder)	1	1	0	1	1	0.8	ใช้ได้	

ภาคผนวก ค

แบบประเมินกรอบกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร สำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

เลขที่แบบประเมิน.....

แบบประเมิน
เรื่อง “การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร สำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์”

คำชี้แจง

แบบสอบถามนี้เป็นส่วนหนึ่งของการวิจัยของนักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม โดยมีวัตถุประสงค์เพื่อศึกษากรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ ผู้วิจัยใคร่ขอความร่วมมือและขอขอบพระคุณท่านในการให้ความกรุณาตอบแบบสอบถามทุกข้อ โดยข้อมูลที่ได้นี้จะได้นำไปใช้ประกอบการศึกษาเพื่อประโยชน์ทางด้านวิชาการเท่านั้น ขอรับรองว่าการตอบแบบสอบถามนี้จะไม่มีผลกระทบหรือก่อให้เกิดความเสียหายต่อตัวท่านแต่ประการใด

แบบสอบถามฉบับนี้ แบ่งเป็น 3 ส่วน ดังนี้

ส่วนที่ 1: ข้อมูลส่วนบุคคลหรือหน่วยงานของผู้ตอบแบบประเมิน

ส่วนที่ 2: ข้อคำถามเกี่ยวกับการประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร

ส่วนที่ 3: ความคิดเห็นและข้อเสนอแนะอื่น ๆ

โปรดพิจารณาข้อคำถามต่อไปนี้แล้วทำเครื่องหมาย ✓ ลงในช่องที่ตรงกับความจริงหรือความคิดเห็น หรือความรู้สึกของท่านมากที่สุดเพียงช่องเดียวแบ่งระดับคำตอบเป็น 5 ระดับ ดังนี้

5	หมายถึง	เป็นจริงหรือเห็นด้วยมากที่สุด
4	หมายถึง	เป็นจริงหรือเห็นด้วยมาก
3	หมายถึง	เป็นจริงหรือเห็นด้วยปานกลาง
2	หมายถึง	เป็นจริงหรือเห็นด้วยน้อย
1	หมายถึง	ไม่เป็นจริงหรือเห็นด้วยน้อยที่สุด

ผู้วิจัย ขอความกรุณาท่านได้ตอบแบบสอบถามตามความเป็นจริงในปัจจุบัน เพื่อให้ได้ข้อมูลที่แท้จริงและสมบูรณ์มากที่สุด ซึ่งการศึกษาวิจัยครั้งนี้จะสรุปออกมาในภาพรวม จะไม่มีผลกระทบต่อท่านและองค์กรแต่อย่างใด

นางสาวฐิติมา ภู่ห้อย E-mail:Thitimaphuhoy@gmail.com โทรศัพท์: 063-156-1466
นักศึกษาหลักสูตรศึกษาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

นิยามศัพท์

วัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ หมายถึง คุณลักษณะ ทัศนคติ ของบุคคลกรและองค์กรเพื่อสนับสนุน เสริมสร้าง รวมทั้งทำให้เกิดความยั่งยืนด้านความมั่นคงปลอดภัยไซเบอร์

การเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ หมายถึง กระบวนการสร้างความตระหนักรู้ด้านความมั่นคง ปลอดภัยไซเบอร์ เป็นการเปลี่ยนทัศนคติและสร้างวัฒนธรรมทางความมั่นคงปลอดภัยไซเบอร์ที่หยั่งรากลึกในระดับบุคคลและองค์กรให้เกิดภูมิคุ้มกัน และมีจริยธรรมทางความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้เพื่อสร้างความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ อีกทั้งยังทำให้บุคคลและองค์กรมีขีดความสามารถด้านไซเบอร์ที่จะป้องกันต่อต้าน ตรวจจับ และตอบสนองต่อการบุกรุก การจารกรรม หรือการหลอกลวง ที่จะทำให้เกิดความเสียหายได้

ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) หมายถึง ภาวะพ้นจากภัยคุกคามที่มีต่อเครือข่าย ระบบคอมพิวเตอร์ โปรแกรม และข้อมูล เพื่อรักษาไว้ซึ่งลักษณะสำคัญ 3 ประการ คือ ความลับ ความถูกต้อง ครบถ้วน และความพร้อมใช้งาน ภาวะดังกล่าวจะเกิดขึ้นได้ต้องอาศัยบุคลากร กระบวนการทำงาน และเครื่องมือที่เหมาะสม

ไซเบอร์ (Cyber) หมายถึง คำที่ใช้เติมหน้าคำอื่นเพื่อแสดงความเกี่ยวข้องกับเครือข่ายคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรืออินเทอร์เน็ต หรือความเป็นจริงเสมือน เช่น ไซเบอร์สเปซ (Cyberspace) หมายถึงสภาพแวดล้อม สมมติในเครือข่ายอินเทอร์เน็ต

ส่วนที่ 1: ข้อมูลส่วนบุคคลหรือหน่วยงานของผู้ตอบแบบสอบถาม

คำชี้แจง โปรดทำเครื่องหมาย ☑ ลงในช่องที่ตรงกับข้อมูลส่วนบุคคลของท่าน

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ ต่ำกว่า 30 ปี ☐ 30-40 ปี

☐ 41-50 ปี ☐ 51-60 ปี

3. ระดับการศึกษาสูงสุด

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี

☐ ปริญญาโท ☐ ปริญญาเอก

4. สายงานที่ปฏิบัติ

☐ ด้านบริหาร ☐ ด้านปฏิบัติการ

☐ ด้านธุรการ ☐ ด้านอื่น ๆ

5. ท่านได้ปฏิบัติงานในหน่วยงานแห่งนี้มานานเท่าใด

☐ ไม่เกิน 5 ปี ☐ 6 – 10 ปี

☐ 11 – 15 ปี ☐ 16 ปีขึ้นไป

6. ท่านได้ใช้เวลาโดยเฉลี่ยอยู่กับคอมพิวเตอร์นานเท่าใด ในแต่ละวันของเวลาทำงาน

☐ น้อยกว่า 1 ชั่วโมงต่อวัน ☐ 1 - 3 ชั่วโมงต่อวัน

☐ 4 – 6 ชั่วโมงต่อวัน ☐ มากกว่า 6 ชั่วโมงต่อวัน

ส่วนที่ 2: ข้อคำถามเกี่ยวกับการประเมินกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร 10 ปัจจัย

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงในช่องที่**ตรงกับความคิดเห็นหรือความรู้สึกของท่านมากที่สุด** เพียงช่องเดียว

ข้อ	รายการประเมิน	ระดับความความคิดเห็น				
		5	4	3	2	1
ปัจจัยที่ 1 นโยบายด้านความมั่นคงปลอดภัยไซเบอร์						
1	องค์กรมีการกำหนดแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์					
2	องค์กรมีการกำหนดหน้าที่ของบุคลากรที่กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์					
3	องค์กรมีการกำหนดระดับสิทธิในการเข้าถึงระบบเครือข่ายของหน่วยงาน					
4	องค์กรมีการกำหนดให้มีการบำรุงรักษาหรือซ่อมแซมอุปกรณ์คอมพิวเตอร์ซึ่งดำเนินการโดยบุคลากรที่ได้รับอนุญาต					
ปัจจัยที่ 2 ผู้นำด้านความมั่นคงปลอดภัยไซเบอร์						
1	องค์กรมีการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์					
2	องค์กรมีการสนับสนุนการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์					
3	องค์กรมีการกำกับดูแลการใช้งานระบบเครือข่ายให้เป็นไปตามแนวปฏิบัติของหน่วยงาน					
4	องค์กรมีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยไซเบอร์					
ปัจจัยที่ 3 การสื่อสารที่ดีด้านความมั่นคงปลอดภัยไซเบอร์						
1	องค์กรมีการเผยแพร่นโยบายและแนวปฏิบัติให้บุคลากรได้รับทราบและปฏิบัติ					
2	องค์กรมีการเผยแพร่แผนการรับมือภัยคุกคามทางไซเบอร์					
3	องค์กรมีการเผยแพร่ความรู้ด้านการรับมือภัยคุกคามทางไซเบอร์					

ข้อ	รายการประเมิน	ระดับความความคิดเห็น				
		5	4	3	2	1
4	องค์กรมีแนวทางให้บุคลากรได้เรียนรู้ประสบการณ์ด้านไซเบอร์ร่วมกัน					
ปัจจัยที่ 4 สมรรถนะของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์						
1	องค์กรมีการการฝึกอบรมสร้างความตระหนักรู้ด้านความปลอดภัย					
2	องค์กรมีการการสนับสนุนบุคลากรในการพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์					
3	บุคลากรสามารถถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยระหว่างกันในองค์กร					
4	บุคลากรมี Cyber Mindset และ Cyber Ethics					
ปัจจัยที่ 5 การจูงใจและการมีส่วนร่วมของบุคลากรในองค์กร						
1	บุคลากรมีความเชื่อมั่นในมาตรการปกป้องข้อมูลส่วนบุคคลในองค์กร					
2	บุคลากรมีความไว้วางใจในระบบเครือข่ายคอมพิวเตอร์ขององค์กร					
3	องค์กรมีอุปกรณ์ในสำนักงานที่สามารถอำนวยความสะดวกในการทำงานได้อย่างมีประสิทธิภาพ					
4	บุคลากรมีความพร้อมและให้ความร่วมมือในการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กร					
ปัจจัยที่ 6 จรรยาบรรณ (Ethical Conduct)						
1	องค์กรมีการกำหนดวิธีรักษาและทำลายข้อมูลขององค์กร					
2	องค์กรมีแนวทางการดำเนินการปกปิดข้อมูลส่วนบุคคล					
3	องค์กรมีแนวปฏิบัติในการรักษาความสมบูรณ์ถูกต้องของข้อมูล					
ปัจจัยที่ 7 มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์						
1	องค์กรมีการตรวจสอบระบบสารสนเทศ (IT Audit)					
2	องค์กรมีการการจัดเก็บข้อมูลจราจร (Log)					
3	องค์กรมีการกำหนดสิทธิระบบเครือข่ายไร้สายให้กับบุคคลภายในและภายนอก					

ข้อ	รายการประเมิน	ระดับความความคิดเห็น				
		5	4	3	2	1
4	องค์กรมีกระบวนการควบคุมการใช้งานอุปกรณ์ส่วนตัวที่มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์					
ปัจจัยที่ 8 การปฏิบัติตามระเบียบและการกำกับดูแล (Compliance and Governance)						
1	องค์กรมีการกำหนดสิทธิ หน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูลของแต่ละส่วนงาน					
2	องค์กรมีการกำหนดนโยบาย/กฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูล					
3	องค์กรมีการกำหนดมาตรการหรือกระบวนการตรวจสอบและประเมินคุณภาพข้อมูล					
4	องค์กรมีมาตรฐานสากลในการบริหารจัดการข้อมูล					
ปัจจัยที่ 9 ความรับผิดชอบและหน้าที่ (Accountability and Responsibility)						
1	องค์กรมีการกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของบุคลากรในหน่วยงาน					
2	องค์กรมีการระบุขั้นตอนและซักซ้อมการแก้ไขปัญหาการบุกรุกระบบเครือข่ายคอมพิวเตอร์					
3	องค์กรมีการแลกเปลี่ยนประสบการณ์ด้านภัยคุกคามทางไซเบอร์					
ปัจจัยที่ 10 ระบบการจัดการด้านความมั่นคงปลอดภัยไซเบอร์						
1	ระบบเครือข่ายขององค์กรมีระบบการยืนยันตัวตน					
2	องค์กรมีการกำหนดสิทธิและระดับในการเข้าถึงข้อมูลหรือระบบต่าง ๆ ของบุคลากร					
3	องค์กรมีระบบจัดเก็บและถ่ายโอนข้อมูลสารสนเทศให้อยู่ในสถานะที่มีความปลอดภัย					
4	องค์กรมีแนวทางการป้องกันและแก้ไขปัญหาการบุกรุกระบบเครือข่าย					

ส่วนที่ 3 : ความคิดเห็นและข้อเสนอแนะอื่น ๆ

.....

.....

.....

.....

ขอขอบพระคุณที่ท่านได้กรุณาเสียสละเวลาในการตอบแบบประเมิน

ภาคผนวก ง

ผลงานตีพิมพ์

การประชุมวิชาการระดับชาติและนานาชาติ ประจำปี 2565
วันที่ 1 กรกฎาคม 2565 ณ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี
SRIPATUM UNIVERSITY AT CHONBURI

ที่ มศป.ชบ 0521.2 / ว 1262

มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี
79 ถนนบางนา-ตราด ตำบลคลองตำหรุ
อำเภอเมือง จังหวัดชลบุรี 20000

21 มิถุนายน 2565

เรื่อง ตอบรับการนำเสนอผลงานทางวิชาการ

เรียน นางสาวฐิติมา ภู่ห้อย

ตามที่ท่านส่งผลงานทางวิชาการเพื่อนำเสนอในประชุมวิชาการระดับชาติ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี ประจำปี 2565 เรื่อง งานวิจัยและนวัตกรรมเพื่อการขับเคลื่อนยุคเศรษฐกิจดิจิทัล วันศุกร์ที่ 1 กรกฎาคม 2565 แบบออนไลน์ ความละเอียดทราบแล้วนั้น

มหาวิทยาลัยฯ ขอแจ้งให้ทราบว่าผลงานทางวิชาการของท่าน ผ่านการประเมินจากผู้ทรงคุณวุฒิ และให้นำเสนอในการประชุมดังกล่าว ท่านสามารถตรวจสอบวัน และเวลาการนำเสนอได้ที่ https://www.chonburi.spu.ac.th/spuccon2022/ ตั้งแต่วันจันทร์ที่ 27 มิถุนายน 2565 เป็นต้นไป

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

(รองศาสตราจารย์กาญจนา มณีแสง)
รองอธิการบดีฝ่ายวิจัยและแผน ปฏิบัติหน้าที่แทน
รองอธิการบดี วิทยาเขตชลบุรี

สำนักงานวิจัยและพัฒนานวัตกรรม
โทรศัพท์ 0-3814-6123 ต่อ 2506, 2507
โทรสาร 0-3814-6011 (ปิดทำการวันอาทิตย์-จันทร์)
e-mail : research@chonburi.spu.ac.th

มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

ขอมอบเกียรติบัตรนี้ไว้เพื่อแสดงว่า

ฐิติมา ภู่ห้อย

ได้นำเสนอผลงานวิชาการภาคบรรยาย

เรื่อง การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

ในการประชุมวิชาการระดับชาติและนานาชาติ ประจำปี 2565 (2022 SPUC National and International Conference)

เรื่อง งานวิจัยและนวัตกรรมเพื่อการขับเคลื่อนยุคเศรษฐกิจดิจิทัล

(Research and Innovation to forward the digital economy era)

วันศุกร์ที่ 1 กรกฎาคม 2565

ณ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

(ดร.บุษบา ชัยจินดา)

รองอธิการบดี วิทยาเขตชลบุรี

ประวัติผู้วิจัย

ชื่อ-สกุล ฐิติมา ภู่ห้อย

วัน เดือน ปีเกิด 16 ธันวาคม 2522

ที่อยู่ปัจจุบัน 47/14 ซอยช่างอากาศอุทิศ 16 แขวง/เขต ดอนเมือง กรุงเทพ 10200

วุฒิการศึกษา พ.ศ. 2545 วิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์
สถาบันราชภัฏจันทรเกษม
พ.ศ. 2565 วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม

ประสบการณ์ทำงาน พ.ศ.2562 - ปัจจุบัน
นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักการวางผังและพัฒนาเมือง
กรุงเทพมหานคร
พ.ศ.2558 – 2562
นักทรัพยากรบุคคลปฏิบัติการ สำนักยุทธศาสตร์และประเมินผล
กรุงเทพมหานคร
พ.ศ.2554 – 2558
นักจัดการงานทั่วไปปฏิบัติการ สำนักป้องกันและบรรเทาสาธารณภัย
กรุงเทพมหานคร
พ.ศ.2551 – 2554
เจ้าหน้าที่บริหารงานทั่วไป ฝ่ายปกครอง สำนักงานเขตดอนเมือง
กรุงเทพมหานคร

สถานที่ทำงานปัจจุบัน สำนักการวางผังและพัฒนาเมือง กรุงเทพมหานคร

ผลงานทางวิชาการที่ได้รับการตีพิมพ์

[1] ฐิติมา ภู่ห้อย, ประสงค์ ปราณีตพลกรัง และสุรชัย ทองแก้ว. **“การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปอลดภัยไซเบอร์”** การประชุมวิชาการระดับชาติและนานาชาติ ประจำปี 2565 เรื่อง งานวิจัยและนวัตกรรมเพื่อการขับเคลื่อนยุคเศรษฐกิจดิจิทัล (Research and Innovation to forward the digital economy era), 1 กรกฎาคม 2565 ณ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี