แนวทางการพัฒนาการปฏิบัติราชการทางอิเล็กทรอนิกส์ ภายใต้กรอบธรรมาภิบาลข้อมูล และความมั่นคงปลอดภัยไซเบอร์: กรณีศึกษา สำนักงานสภาความมั่นคงแห่งชาติ*

Development of Guidelines for Digital Government Operations under Data Governance and Cybersecurity Frameworks: A Case Study of the Office of the National Security Council

สุรเชษฐ์ ริทธิโต[1]

Surachad Rittito

6714832015@rumail.ru.ac.th

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ (1) ศึกษาการปฏิบัติราชการทางอิเล็กทรอนิกส์บนระบบบริหารจัดการสำนักงาน (e-Office) ภายใต้กรอบธรรมาภิบาลข้อมูลและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ (2) ศึกษาปัญหา อุปสรรค และปัจจัยเสี่ยงที่ส่งผลต่อการปฏิบัติราชการทางอิเล็กทรอนิกส์บนระบบบริหารจัดการสำนักงาน (e-Office) และ (3) ศึกษาแนวทางการพัฒนาและปรับปรุงการปฏิบัติราชการทางอิเล็กทรอนิกส์บนระบบบริหารจัดการสำนักงาน (e-Office) เป็นการวิจัยเชิงคุณภาพ เก็บรวบรวมข้อมูลด้วยการวิจัยเอกสารและการสัมภาษณ์แบบกึ่งโครงสร้างจากผู้ให้ข้อมูลสำคัญ จำนวน 5 คน ผลการวิจัยพบว่า ระบบบริหารจัดการสำนักงาน (e-Office) รองรับกระบวนงานสารบรรณได้ค่อนข้างสมบูรณ์ การลงนามด้วยลายมือชื่ออิเล็กทรอนิกส์เป็นไปตามมาตรฐานที่กฎหมายกำหนด หน่วยงานมีคณะกรรมการและนโยบายธรรมาภิบาลข้อมูล กำหนดสิทธิการเข้าถึงตามบทบาทหน้าที่ ส่วนความมั่นคงปลอดภัยไซเบอร์มีลักษณะเป็นความรับผิดชอบร่วมกับเจ้าของระบบ ยกเว้นแต่ เอกสารชั้นความลับสูงและเอกสารทางการคลังยังคงดำเนินการในรูปแบบกระดาษ ส่วนปัญหา อุปสรรค และปัจจัยเสี่ยงจำแนกได้ 4 ด้าน ได้แก่ ด้านเทคโนโลยี ด้านบุคลากร ด้านกระบวนการ และด้านการกำกับดูแล การปฏิบัติงานยังเคยชินกับรูปแบบการทำงานเดิม และแนวทางการพัฒนาควรกำหนดแนวปฏิบัติการใช้งานให้เป็นเอกภาพ ยกระดับธรรมาภิบาลข้อมูลสู่การใช้ข้อมูลเชิงวิเคราะห์ การบังคับใช้การยืนยันตัวตนแบบหลายปัจจัยและการจัดทำข้อตกลงระดับการให้บริการร่วมกับเจ้าของระบบ ตลอดจนการขับเคลื่อนเชิงองค์กรโดยบทบาทนำของผู้บริหาร

คำสำคัญ: การปฏิบัติราชการทางอิเล็กทรอนิกส์; ธรรมาภิบาลข้อมูล; ความมั่นคงปลอดภัยไซเบอร์

Keywords: Digital Government Operations; Data Governance; Cybersecurity

---

*บทความนี้เรียบเรียงจากการค้นคว้าอิสระเรื่อง แนวทางการพัฒนาการปฏิบัติราชการทางอิเล็กทรอนิกส์ภายใต้กรอบธรรมาภิบาลข้อมูลและความมั่นคงปลอดภัยไซเบอร์: กรณีศึกษา สำนักงานสภาความมั่นคงแห่งชาติ

[1]นักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะรัฐศาสตร์ มหาวิทยาลัยรามคำแหง

บทนำ

ปัจจุบันการบริหารราชการแผ่นดินได้ก้าวเข้าสู่ยุคที่เทคโนโลยีสารสนเทศและการสื่อสารกลายเป็นโครงสร้างพื้นฐานสำคัญของการบริหารราชการสมัยใหม่ องค์การสหประชาชาติชี้ว่าการพัฒนารัฐบาลอิเล็กทรอนิกส์ (e-Government) เป็นกลไกสำคัญในการเสริมสร้างธรรมาภิบาล ความโปร่งใส และการมีส่วนร่วมของประชาชน (United Nations, 2022) สำหรับประเทศไทยได้ขับเคลื่อนการปฏิรูปการบริหารราชการสู่ยุคดิจิทัลอย่างต่อเนื่องภายใต้ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561–2580) (สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, 2561) และแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2566–2570 (สำนักงานพัฒนารัฐบาลดิจิทัล, 2566) โดยมีพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 เป็นแรงผลักดันสำคัญที่กำหนดให้หน่วยงานของรัฐต้องจัดให้มีระบบการปฏิบัติราชการในรูปแบบอิเล็กทรอนิกส์ และรับรองผลทางกฎหมายของการดำเนินการในรูปแบบดิจิทัลให้เทียบเท่าการดำเนินการบนกระดาษ ทั้งนี้ การขับเคลื่อนดังกล่าวถือเป็นส่วนหนึ่งของการปฏิรูประบบราชการ ซึ่งหมายถึงการปรับเปลี่ยนพื้นฐานของระบบราชการหรือองค์การสาธารณะโดยเพิ่มประสิทธิภาพ ประสิทธิผล ความสามารถในการปรับตัว และการคิดค้นสิ่งใหม่ ๆ (Hammer & Champy, 1993, อ้างถึงใน วิโรจน์ ก่อสกุล, 2568) และเป็นการสร้างนวัตกรรมทางการบริหารซึ่งจำเป็นต้องอาศัยความเข้าใจและความร่วมมือจากทุกฝ่ายที่มีส่วนเกี่ยวข้องกับการเปลี่ยนแปลง (Drucker, 1995, อ้างถึงใน วิโรจน์ ก่อสกุล, 2568)

สำนักงานสภาความมั่นคงแห่งชาติ (สมช.) ในฐานะฝ่ายเลขานุการของสภาความมั่นคงแห่งชาติมีภารกิจในการรวบรวม วิเคราะห์ และประมวลข้อมูลข่าวสารที่มีความละเอียดอ่อนสูงซึ่งกระทบต่อความมั่นคงของรัฐ ทั้งยังมีสถานะเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ด้านความมั่นคงของรัฐ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 การนำระบบบริหารจัดการสำนักงานอิเล็กทรอนิกส์ (e-Office) มาใช้ในองค์กรลักษณะนี้จึงมีความซับซ้อนและความเสี่ยงแตกต่างจากหน่วยงานราชการทั่วไป เนื่องจากต้องเผชิญภัยคุกคามทางไซเบอร์ระดับสูง ทั้งการแทรกแซงข้อมูลข่าวสารจากต่างชาติ (Foreign Information Manipulation and Interference: FIMI) การโจมตีแบบขั้นสูง (Advanced Persistent Threat: APT) และการบิดเบือนข้อมูลด้วยเทคโนโลยีปัญญาประดิษฐ์ การปฏิบัติราชการทางอิเล็กทรอนิกส์ของสำนักงานสภาความมั่นคงแห่งชาติจึงต้องบูรณาการกรอบธรรมาภิบาลข้อมูลภาครัฐ (สำนักงานพัฒนารัฐบาลดิจิทัล, 2566) เข้ากับมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกรอบการรักษาความปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National institute of Standards and Technology: NIST) หรือ NIST Cybersecurity Framework และมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศหรือมาตรฐาน ISO/IEC 27001 ซึ่งจัดทำโดยองค์การระหว่างประเทศว่าด้วยการมาตรฐาน (International Organization for Standardization: ISO) และคณะกรรมาธิการระหว่างประเทศด้านมาตรฐานสาขาวิศวกรรมอิเล็กทรอนิกส์ (International Electrotechnical Commission: IEC) ตลอดจนกฎหมายที่เกี่ยวข้อง อาทิ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564

จากการทบทวนวรรณกรรมพบว่า งานวิจัยในประเทศส่วนใหญ่ศึกษาการนำระบบสารบรรณอิเล็กทรอนิกส์มาใช้ในหน่วยงานภาครัฐ (เนตรชนก สุขสวัสดิ์, 2565; มานิตย์ กุศลคุ้ม, 2562) หรือศึกษาการจัดการความเสี่ยงด้านไซเบอร์ของหน่วยงานภาครัฐเป็นรายมิติ ขณะที่งานวิจัยต่างประเทศก็มักศึกษากรอบธรรมาภิบาลข้อมูลและกรอบความมั่นคงปลอดภัยไซเบอร์แยกจากกัน (Alsaad, 2023) และยังขาดงานวิจัยที่บูรณาการทั้งสองมิติเข้าด้วยกันในบริบทของหน่วยงานด้านความมั่นคงแห่งชาติซึ่งมีสถานะเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) การวิจัยครั้งนี้จึงมุ่งเติมเต็มช่องว่างดังกล่าว โดยมีวัตถุประสงค์เพื่อ (1) ศึกษาการปฏิบัติราชการทางอิเล็กทรอนิกส์บนระบบบริหารจัดการสำนักงาน (e-Office) ภายใต้กรอบ

ธรรมาภิบาลข้อมูลและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ (2) ศึกษาปัญหา อุปสรรค และปัจจัยเสี่ยง (Risk Factors) ที่ส่งผลต่อการปฏิบัติราชการทางอิเล็กทรอนิกส์บนระบบบริหารจัดการสำนักงาน (e-Office) และ (3) ศึกษาแนวทางการพัฒนาและปรับปรุงการปฏิบัติราชการทางอิเล็กทรอนิกส์บนระบบบริหารจัดการสำนักงาน (e-Office) ของสำนักงานสภาความมั่นคงแห่งชาติ

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) ประกอบด้วยวิธีการวิจัย 2 ส่วน ได้แก่ (1) การวิจัยเอกสาร (Documentary Research) โดยศึกษาจากกฎหมาย ระเบียบ มาตรฐาน กรอบแนวปฏิบัติด้านธรรมาภิบาลข้อมูลและความมั่นคงปลอดภัยไซเบอร์ ตลอดจนเอกสารและแนวปฏิบัติภายในของสำนักงานสภาความมั่นคงแห่งชาติที่เกี่ยวข้องกับการปฏิบัติราชการทางอิเล็กทรอนิกส์ และ (2) การวิจัยสนาม (Field Research) โดยการสัมภาษณ์แบบกึ่งโครงสร้าง (Semi-structured Interview)

ประชากรและผู้ให้ข้อมูลสำคัญ

การวิจัยครั้งนี้ มีประชากรและผู้ให้ข้อมูลสำคัญ ดังนี้

1. ประชากร (Population) ของการวิจัย ได้แก่ ข้าราชการและเจ้าหน้าที่ผู้ปฏิบัติงานของสำนักงานสภาความมั่นคงแห่งชาติ ที่มีส่วนเกี่ยวข้องกับการปฏิบัติราชการทางอิเล็กทรอนิกส์บนระบบบริหารจัดการสำนักงาน (e-Office) โดยเฉพาะบุคลากรของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

2. ผู้ให้ข้อมูลสำคัญ (Key Informants) ได้มาจากการเลือกแบบเจาะจง (Purposive Sampling) จำนวน 5 คน ซึ่งเป็นข้าราชการและเจ้าหน้าที่ของสำนักงานสภาความมั่นคงแห่งชาติที่เกี่ยวข้องโดยตรงกับระบบบริหารจัดการสำนักงาน (e-Office) ครอบคลุมผู้บริหาร ผู้กำกับดูแลเชิงนโยบายด้านเทคโนโลยีสารสนเทศ ผู้วิเคราะห์ยุทธศาสตร์ด้านดิจิทัลและความมั่นคงปลอดภัยไซเบอร์ ผู้ดูแลระบบ และผู้ใช้งานระดับปฏิบัติการจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานสภาความมั่นคงแห่งชาติ ซึ่งเอื้อต่อการตรวจสอบข้อมูลแบบสามเส้าด้านผู้ให้ข้อมูล (Data Source Triangulation) ดังนี้

2.1 ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

2.2 เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

2.3 นักวิชาการคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

2.4 เจ้าหน้าที่วิเคราะห์นโยบายและแผน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

2.5 นักวิเคราะห์นโยบายและแผน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการวิจัย คือ แบบสัมภาษณ์แบบกึ่งโครงสร้างซึ่งกำหนดประเด็นคำถามตามวัตถุประสงค์การวิจัย 3 ส่วน ได้แก่ กระบวนการหลักของระบบบริหารจัดการสำนักงาน (e-Office) และการปฏิบัติตามกรอบธรรมาภิบาลข้อมูลและความมั่นคงปลอดภัยไซเบอร์ ปัญหา อุปสรรค และปัจจัยเสี่ยงใน 4 มิติ และแนวทางการพัฒนาปรับปรุง ในการเก็บรวบรวมข้อมูล ผู้วิจัยชี้แจงวัตถุประสงค์และขออนุญาตจดบันทึกและบันทึกเสียงทุกครั้ง โดยดำเนินการภายใต้กรอบการรักษาความลับของทางราชการอย่างเคร่งครัด และไม่นำข้อมูลที่มีชั้นความลับมาเปิดเผยในผลการวิจัย

การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลใช้การวิเคราะห์เนื้อหา (Content Analysis) และการวิเคราะห์แบบจัดกลุ่มประเด็น (Thematic Analysis) โดยใช้กรอบวิเคราะห์เชิงทฤษฎี 3 กรอบเป็นแนวทางในการจัดระเบียบและตีความข้อมูล ได้แก่ กรอบธรรมาภิบาลข้อมูลภาครัฐของสำนักงานพัฒนารัฐบาลดิจิทัล กรอบการรักษาความปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National institute of Standards and Technology: NIST) และมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศหรือมาตรฐาน ISO/IEC 27001 ซึ่งจัดทำโดยองค์การระหว่างประเทศว่าด้วยการมาตรฐาน (International Organization for Standardization: ISO) และคณะกรรมาธิการระหว่างประเทศด้านมาตรฐานสาขาวิศวกรรมอิเล็กทรอนิกส์ (International Electrotechnical Commission: IEC) และกรอบกฎหมายและระเบียบที่เกี่ยวข้อง แล้วสังเคราะห์สร้างข้อสรุปแบบอุปนัย (Analytic Induction) นำเสนอผลในรูปแบบการพรรณนาวิเคราะห์

ผลการวิจัยและอภิปรายผล

ผลการวิจัยนำเสนอตามวัตถุประสงค์ของการวิจัย 3 ประการ ดังนี้

1. การปฏิบัติราชการทางอิเล็กทรอนิกส์บนระบบบริหารจัดการสำนักงาน (e-Office) ภายใต้กรอบธรรมาภิบาลข้อมูลและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์

สำนักงานสภาความมั่นคงแห่งชาติได้นำระบบบริหารจัดการสำนักงาน (e-Office) ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ภายใต้บริการคลาวด์กลางภาครัฐ (Government Data Center and Cloud Service: GDCC) มาใช้ในการปฏิบัติราชการตั้งแต่วันที่ 2 มกราคม 2568 โดยเปิดใช้งานระบบย่อยหลัก 3 ระบบ ได้แก่ ระบบพิมพ์ร่างตรวจหนังสือ (Draft) ระบบลงนามด้วยลายมือชื่ออิเล็กทรอนิกส์ (In-tray) และระบบสารบรรณอิเล็กทรอนิกส์ (e-Saraban) ผลการศึกษาพบว่าระบบรองรับกระบวนงานสารบรรณภายในหน่วยงานได้ค่อนข้างราบรื่น ดังที่ผู้ให้ข้อมูลสำคัญคนที่ 4 (2569) ในฐานะผู้ใช้งานระดับปฏิบัติที่ให้ข้อมูลว่า “...รองรับกระบวนการปฏิบัติงานด้านสารบรรณอิเล็กทรอนิกส์ได้อย่างครบถ้วน ตั้งแต่การร่างเอกสาร การเสนอและตรวจสอบตามลำดับชั้น การพิจารณาอนุมัติ การรับ-ส่งหนังสือ ตลอดจนการแจ้งเวียนเอกสารภายในหน่วยงาน ส่งผลให้การดำเนินงานมีความสะดวกรวดเร็ว และสามารถติดตามสถานะของเอกสารได้อย่างต่อเนื่อง” โดยการอนุมัติและการลงนามด้วยลายมือชื่ออิเล็กทรอนิกส์เป็นไปตามมาตรฐานที่กฎหมายกำหนด สอดคล้องกับพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 และระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 อีกทั้งผู้ส่งและผู้รับสามารถติดตามสถานะและเส้นทางของเอกสารได้แบบ Real-time ภายในระบบ ซึ่งเสริมสร้างความโปร่งใสและความสามารถในการตรวจสอบ อย่างไรก็ตามยังมีกระบวนการที่ต้องใช้เอกสารกระดาษควบคู่ 4 กลุ่ม ได้แก่ เอกสารการอนุมัติค่าใช้จ่ายและการเบิกจ่ายงบประมาณ เอกสารที่ต้องลงนามมากกว่าหนึ่งจุด การตรวจทานแก้ไขร่างหนังสือบางกรณี และเอกสารที่มีชั้นความลับสูง

ด้านธรรมาภิบาลข้อมูล หน่วยงานมีกลไกที่เป็นรูปธรรม โดยจัดตั้งคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee) และประกาศใช้นโยบายธรรมาภิบาลข้อมูลที่จัดทำตามกรอบธรรมาภิบาลข้อมูลภาครัฐของสำนักงานพัฒนารัฐบาลดิจิทัล ครอบคลุมการจัดหมวดหมู่และชั้นความลับของเอกสาร การบริหารจัดการข้อมูลตามวงจรชีวิต การพัฒนาคุณภาพข้อมูล และการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล มีการจำแนกแฟ้มรับ-ส่งเป็นแฟ้มเอกสารทั่วไปและแฟ้มเอกสารลับ โดยเอกสารลับต้องกำหนดรหัสผ่านให้ไฟล์ก่อนนำเข้าระบบ ส่วนข้อมูลชั้นลับที่สุดไม่อนุญาตให้นำเข้าสู่ระบบสารบรรณอิเล็กทรอนิกส์ ต้องดำเนินการตามระเบียบว่าด้วยการรักษาความลับของทางราชการเท่านั้น การกำหนดสิทธิการเข้าถึงใช้หลักการตามบทบาทหน้าที่ (Role-Based Access Control: RBAC) ภายใต้หลักการจำกัดสิทธิ์เท่าที่จำเป็น (Need-to-Know Basis)

ทั้งนี้ ผู้ให้ข้อมูลสำคัญระดับบริหารและระดับนโยบายให้ข้อมูลตรงกันว่า ปัจจุบันหน่วยงานยังจำกัดการใช้งานระบบเฉพาะเอกสารทั่วไปและเอกสารเวียน เนื่องจากมีข้อกังวลเรื่องความเสี่ยงจากการรั่วไหลของข้อมูล ดังที่ผู้ให้ข้อมูลสำคัญคนที่ 1 (2569) ที่ให้ข้อมูลว่า "ในปัจจุบันยังไม่ได้นำระบบมาใช้กับเอกสารที่มีชั้นความลับ เนื่องจากมีข้อกังวลในเรื่องการรั่วไหลของข้อมูล" และผู้ให้ข้อมูลสำคัญคนที่ 2 (2569) ที่ให้ข้อมูลว่า "ข้อมูลที่มีชั้นความลับสูงของ สมช. จะต้องถูกแยกออกไปดำเนินการตามระเบียบว่าด้วยการรักษาความลับของทางราชการ ผ่านระบบเครือข่ายเฉพาะหรือเอกสารกระดาษที่เป็นความลับเท่านั้น เพื่อป้องกันความเสี่ยงจากการรั่วไหลของข้อมูล"

ด้านความมั่นคงปลอดภัยไซเบอร์ เมื่อวิเคราะห์ตามหน้าที่หลัก 5 ด้านของกรอบการรักษาความปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology: NIST) พบว่ามาตรการมีลักษณะเป็นความรับผิดชอบร่วม (Shared Responsibility) กล่าวคือ เจ้าของระบบรับผิดชอบโครงสร้างพื้นฐาน การเข้ารหัสข้อมูล การสำรองข้อมูล และการเฝ้าระวังระดับแอปพลิเคชันภายใต้มาตรฐาน ISO/IEC 27001 ส่วนสำนักงานสภาความมั่นคงแห่งชาติในฐานะหน่วยงานผู้ใช้งานรับผิดชอบทะเบียนทรัพย์สินสารสนเทศของอุปกรณ์ปลายทาง การยืนยันตัวตนผู้ใช้ การกำหนดสิทธิ์ การเฝ้าระวังเครือข่ายภายในและบันทึกการใช้งาน การฝึกอบรมสร้างความตระหนักรู้ ตลอดจนแผนเผชิญเหตุ ดังปรากฏชัดในมิติการระบุ (Identify) ที่ผู้ให้ข้อมูลสำคัญคนที่ 2 (2569) ที่ให้ข้อมูลว่า "มีการจัดทำทะเบียนทรัพย์สินสารสนเทศ (Asset Inventory) ในส่วนที่เป็นอุปกรณ์ปลายทาง เช่น คอมพิวเตอร์และระบบเครือข่ายภายใน สมช. แต่ในส่วนของระบบ e-Office และเครื่องแม่ข่ายหลักนั้น ทรัพย์สินและสถาปัตยกรรมระบบจะถูกระบุและประเมินความเสี่ยงโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและผู้ให้บริการ Cloud GDCC เป็นหลัก" ในทำนองเดียวกัน มิติการตรวจจับ (Detect) เป็นหน้าที่ของผู้ให้บริการคลาวด์ในระดับระบบปฏิบัติการและแอปพลิเคชัน ขณะที่หน่วยงานเฝ้าระวังในระดับเครือข่ายภายในและบันทึกการใช้งาน มิติการป้องกัน (Protect) หน่วยงานรับผิดชอบการยืนยันตัวตนด้วยชื่อบัญชีและรหัสผ่าน การเชื่อมโยงกับระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล และอยู่ระหว่างปรับเปลี่ยนสู่การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) มิติการตอบสนอง (Respond) มีแผนเผชิญเหตุและทีมรักษาความมั่นคงปลอดภัยไซเบอร์เป็นผู้รับผิดชอบหลัก ส่วนมิติการฟื้นฟู (Recover) เป็นความรับผิดชอบหลักของผู้ให้บริการคลาวด์กลางภาครัฐ โดยหน่วยงานมีแนวทางรองรับสถานการณ์ฉุกเฉินและทำหน้าที่ประสานติดตามการแก้ไขปัญหาจนระบบกลับมาให้บริการได้ตามปกติ

2. ปัญหา อุปสรรค และปัจจัยเสี่ยงที่ส่งผลต่อการปฏิบัติราชการทางอิเล็กทรอนิกส์บนระบบบริหารจัดการสำนักงาน (e-Office) ผลการวิจัยจำแนกปัญหา อุปสรรค และปัจจัยเสี่ยงได้ 4 ด้าน ดังนี้

2.1 ด้านเทคโนโลยี พบปัญหาความมีเสถียรของระบบและความล่าช้าในการประมวลผล การเชื่อมต่อระบบอีเมลกลางของหน่วยงานกับระบบที่ยังติดขัด ข้อจำกัดในการรองรับอุปกรณ์เคลื่อนที่ และข้อจำกัดด้านฟังก์ชันและการบูรณาการข้อมูล ซึ่งการส่งผ่านข้อมูลข้ามหน่วยงานยังเป็นลักษณะเอกสารแนบ ขาดการเชื่อมโยงระดับชุดข้อมูล

2.2 ด้านบุคลากร พบว่าผู้ให้ข้อมูลสำคัญทุกคนระบุตรงกันว่า ความเคยชินกับรูปแบบการทำงานเดิมเป็นอุปสรรคสำคัญที่สุดด้านบุคลากร ดังผู้ให้ข้อมูลสำคัญคนที่ 2 (2569) ที่ให้ข้อมูลว่า "บุคลากรบางส่วนยังมีความเคยชินกับการอ่านและตรวจแก้เอกสารบนกระดาษ ทำให้เกิดภาวะทำงานซ้ำซ้อน กล่าวคือ คีย์ข้อมูลเข้าระบบ พิมพ์ออกมาตรวจ แก้ไข แล้วคีย์เข้าระบบใหม่" ประกอบกับข้อจำกัดด้านทักษะดิจิทัลเชิงลึก ความไม่เพียงพอของบุคลากรด้านเทคนิค และความเสี่ยงจากองค์ความรู้ที่ผูกติดกับตัวบุคคล

2.3 ด้านกระบวนการ พบความยากในการตรวจแก้และให้ความเห็นต่อเอกสารบนระบบ ความไม่ชัดเจนของทิศทางการใช้งาน ดังที่ผู้ให้ข้อมูลสำคัญคนที่ 3 (2569) ที่ให้ข้อมูลว่า "ปัญหาเรื่องการไม่ได้กำหนดทิศทางการใช้งานให้ชัดเจน เนื่องจากระบบมีความยืดหยุ่นในการใช้งาน เพราะถูกออกแบบมาให้

ทุกหน่วยงานสามารถใช้ร่วมกันได้ จนมีทางเลือกให้ผู้ใช้มากเกินไป ทำให้ทิศทางการใช้งานของระบบในแต่ละส่วนงานไม่ได้ไปในทิศทางเดียวกัน" ทำให้แต่ละส่วนงานปฏิบัติแตกต่างกันและเกิดความสับสนในการประสานงาน นอกจากนี้ ยังพบข้อจำกัดของฟังก์ชันการลงนามและการจัดทำเอกสาร ตลอดจนเส้นทางการอนุมัติ (Workflow) ที่ไม่ยืดหยุ่นเพียงพอต่อการกลั่นกรองเอกสารยุทธศาสตร์ความมั่นคง ทำให้เจ้าหน้าที่ต้องสลับการทำงานระหว่างกระบวนการอิเล็กทรอนิกส์กับกระบวนการดั้งเดิมสำหรับเอกสารลับ

2.4 ด้านการกำกับดูแล พบโครงสร้างความรับผิดชอบที่ทับซ้อนระหว่างเจ้าของข้อมูล (Data Owner) กับผู้ประมวลผลข้อมูล (Data Processor) ดังที่ผู้ให้ข้อมูลสำคัญคนที่ 2 (2569) ที่ให้ข้อมูลว่า "เนื่องจากเป็นระบบของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมที่ติดตั้งอยู่บน Cloud GDCC แต่ข้อมูลเป็นของ สมช. ทำให้เกิดความไม่ชัดเจนในขอบเขตความรับผิดชอบด้านความปลอดภัยข้อมูล ระหว่างความเป็นเจ้าของข้อมูล (Data Ownership) กับผู้ประมวลผลข้อมูล (Data Processor)" และความท้าทายในการบังคับใช้มาตรการและการขับเคลื่อนการเปลี่ยนแปลงซึ่งเผชิญแรงต้านตามธรรมชาติจากความคุ้นชินในวิถีการทำงานเดิม

3. แนวทางการพัฒนาและปรับปรุงการปฏิบัติราชการทางอิเล็กทรอนิกส์บนระบบบริหารจัดการสำนักงาน (e-Office) แนวทางการพัฒนาที่สังเคราะห์ได้จำแนกเป็น 4 กลุ่ม ดังนี้

3.1 การพัฒนากระบวนการหลักของระบบ หน่วยงานควรกำหนดแนวปฏิบัติมาตรฐาน (Standard Operating Procedure: SOP) ที่เป็นเอกภาพสำหรับทุกกระบวนการสำคัญ ซึ่งเป็นข้อเสนอที่สอดคล้องกันทั้งจากฝ่ายผู้ดูแลระบบและฝ่ายผู้ใช้งาน ดังที่ผู้ให้ข้อมูลสำคัญคนที่ 5 (2569) ที่ให้ข้อมูลว่า "ควรจัดทำคู่มือหรือแนวปฏิบัติมาตรฐาน (SOP) ที่ชัดเจน พร้อมการอบรมและประชาสัมพันธ์ให้ผู้ใช้ทราบอย่างทั่วถึง เพื่อลดความสับสนและความคลาดเคลื่อนในการใช้งาน และทำให้ทุกส่วนงานปฏิบัติงานไปในทิศทางเดียวกัน" ควบคู่กันควรประสานผลักดันเจ้าของระบบให้ปรับปรุงฟังก์ชันให้สอดคล้องกับการปฏิบัติงานจริง และเปิดช่องทางเชื่อมต่อเพื่อประยุกต์ใช้ปัญญาประดิษฐ์และระบบอัตโนมัติในการคัดแยกหนังสือเวียน สรุปสาระสำคัญของเอกสารแนบ และร่างหนังสือตอบกลับเบื้องต้น ตลอดจนพัฒนาการใช้งานบนอุปกรณ์เคลื่อนที่ให้เสถียรและปลอดภัยยิ่งขึ้น

3.2 การพัฒนาด้านธรรมาภิบาลข้อมูล ควรเร่งรัดจัดทำพจนานุกรมข้อมูล (Data Dictionary) และคำอธิบายชุดข้อมูล (Metadata) เพื่อยกระดับจากการจัดเก็บเอกสารเพื่อการสืบค้นไปสู่การใช้ข้อมูลเพื่อการวิเคราะห์ ดังที่ผู้ให้ข้อมูลสำคัญคนที่ 2 (2569) ที่ให้ข้อมูลว่า "ควรเร่งรัดการจัดทำพจนานุกรมข้อมูล (Data Dictionary) และเมทาดาตาสำหรับเอกสารที่ผ่านการพิจารณาของผู้บริหารแล้ว เพื่อแปลงเอกสารที่นิ่งอยู่เฉย ๆ ในคลัง ให้กลายเป็นชุดข้อมูลที่มีโครงสร้าง (Structured Data) ซึ่งจะช่วยให้ สมช. สามารถนำข้อมูลเอกสารนโยบายเหล่านี้ไปใช้ประโยชน์ในการสืบค้นเชิงลึก หรือใช้เป็นฐานข้อมูลในการวิเคราะห์แนวโน้มยุทธศาสตร์ความมั่นคงในอนาคตได้" นอกจากนี้ควรออกแบบระบบจัดการข้อมูลที่รองรับการประยุกต์ใช้ปัญญาประดิษฐ์อย่างปลอดภัยควบคู่กับการคุ้มครองข้อมูลส่วนบุคคล และขับเคลื่อนกลไกธรรมาภิบาลข้อมูลให้ครบวงจร

3.3 การยกระดับมาตรการความมั่นคงปลอดภัยไซเบอร์ ผู้ให้ข้อมูลสำคัญทุกระดับเสนอตรงกันให้เร่งรัดการบังคับใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) ควบคู่กับการจัดทำข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) และขั้นตอนการปฏิบัติงานมาตรฐานร่วม (Joint SOP) กับเจ้าของระบบ เพื่อลดช่องว่างด้านเวลาในการเผชิญเหตุไซเบอร์ ดังที่ผู้ให้ข้อมูลสำคัญคนที่ 2 (2569) ที่ให้ข้อมูลว่า "...สิทธิ์ในการระงับบัญชีผู้ใช้บนระบบ e-Office ยังต้องพึ่งพาผู้ดูแลระบบของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สมช. จึงควรผลักดันให้มีการจัดทำขั้นตอนการปฏิบัติงานมาตรฐานร่วม (Joint SOP) ที่ระบุช่องทางการประสานงานฉุกเฉินตลอด 24 ชั่วโมง หรือการขอสิทธิ์ระดับผู้ดูแลระบบย่อย เพื่อให้เจ้าหน้าที่เทคนิคของ สมช. สามารถระงับบัญชีที่เกิดเหตุได้เองทันที

ในกรณีวิกฤต” นอกจากนี้ ควรจัดการทดสอบเจาะระบบเชิงรุก และเตรียมความพร้อมด้านการเข้ารหัสที่ต้านทานเทคโนโลยีควอนตัม

3.4 การขับเคลื่อนเชิงองค์กร ควรเรียนรู้จากหน่วยงานต้นแบบด้านการเบิกจ่ายอิเล็กทรอนิกส์ จัดตั้งทีมทบทวนและติดตามการใช้งานระบบเพื่อแก้ปัญหาองค์ความรู้ที่ผูกติดกับตัวบุคคล และรับฟังเสียงสะท้อนจากผู้ใช้งานอย่างต่อเนื่อง ทั้งนี้ ปัจจัยชี้ขาดอยู่ที่การสร้างแรงจูงใจและบทบาทนำของผู้บริหาร ดังที่ผู้ให้ข้อมูลสำคัญคนที่ 4 (2569) ที่ให้ข้อมูลว่า “การขับเคลื่อน...ควรเริ่มจากการสร้างแรงจูงใจและความตระหนักรู้ให้แก่เจ้าหน้าที่ของ สมช. เพื่อให้เห็นถึงความสำคัญและประโยชน์ของการนำเทคโนโลยีมาประยุกต์ใช้ โดยเฉพาะผู้บริหาร ซึ่งมีบทบาทสำคัญในการกำหนดทิศทางและผลักดันการใช้งานระบบให้เกิดขึ้นอย่างเป็นรูปธรรม ควบคู่กับการกำหนดนโยบายและแนวปฏิบัติที่มีความเป็นเอกภาพ” สำหรับระยะยาว มีข้อเสนอเชิงยุทธศาสตร์ให้พิจารณาพัฒนาระบบบริหารจัดการข้อมูลและการทำงานอิเล็กทรอนิกส์ภายในที่มั่นคงปลอดภัย (Secure Internal Work Platform) สำหรับเอกสารชั้นความลับ

การอภิปรายผล

จากผลการวิจัยเรื่อง แนวทางการพัฒนาการปฏิบัติราชการทางอิเล็กทรอนิกส์ภายใต้กรอบธรรมาภิบาลข้อมูลและความมั่นคงปลอดภัยไซเบอร์: กรณีศึกษา สำนักงานสภาความมั่นคงแห่งชาติ ซึ่งเป็นการวิจัยเชิงคุณภาพที่เก็บรวบรวมข้อมูลด้วยการวิจัยเอกสารควบคู่กับการสัมภาษณ์แบบกึ่งโครงสร้างจากผู้ให้ข้อมูลสำคัญ จำนวน 5 คน ครอบคลุมทั้งระดับบริหาร ระดับนโยบายและความมั่นคงปลอดภัยไซเบอร์ ระดับผู้ดูแลระบบ และระดับผู้ใช้งานปฏิบัติการ ผู้วิจัยพบว่ามีประเด็นสำคัญหลายประการที่ควรค่าแก่การนำมาอภิปราย ทั้งประเด็นที่มีความสอดคล้องกับแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง และประเด็นที่สะท้อนลักษณะเฉพาะของหน่วยงานด้านความมั่นคงแห่งชาติซึ่งมีสถานะเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) อันแตกต่างไปจากหน่วยงานราชการทั่วไป ผู้วิจัยจึงนำผลการวิจัยมาอภิปรายโดยเชื่อมโยงกับแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง จำแนกตามวัตถุประสงค์ของการวิจัยทั้ง 3 ประการ ดังนี้

จากผลการวิจัยตามวัตถุประสงค์ข้อ 1. นำมาอภิปรายได้ดังนี้

1. **การนำระบบบริหารจัดการสำนักงาน (e-Office) มาใช้สะท้อนการปฏิรูประบบราชการสู่ยุคดิจิทัลตามแนวคิดการจัดการภาครัฐแนวใหม่ภายใต้เงื่อนไขสมดุลเฉพาะของหน่วยงานความมั่นคง** ผลการวิจัยที่พบว่าสำนักงานสภาความมั่นคงแห่งชาตินำระบบบริหารจัดการสำนักงาน (e-Office) มาใช้แทนที่กระบวนการทำงานแบบกระดาษ เพื่อเพิ่มประสิทธิภาพ ลดระยะเวลา และสร้างความรับผิดชอบที่ตรวจสอบได้ ซึ่งสอดคล้องกับแนวคิดการจัดการภาครัฐแนวใหม่ (New Public Management: NPM) ที่เน้นการนำวิธีการบริหารจัดการภาคเอกชนมาประยุกต์ใช้โดยยึดผลลัพธ์เป็นสำคัญ และแนวคิดการบริหารยุคดิจิทัล (Digital Era Governance) ที่เน้นการทำให้กระบวนการเป็นดิจิทัล (Dunleavy, Margetts, Bastow, & Tinkler, 2006) ทั้งนี้สาระสำคัญของการบริหารจัดการภาครัฐแนวใหม่อยู่ที่การให้ความสำคัญกับระบบการจัดการยิ่งกว่าตัวนโยบาย โดยเน้นที่ผลงานและประสิทธิภาพเป็นหลัก (วสันต์ เหลืองประภัสร์, 2548, อ้างถึงใน ปะการัง ชื่นจิต, 2568) และเป็นการสร้างนวัตกรรมทางการบริหารซึ่งต้องอาศัยความเข้าใจและความร่วมมือจากทุกฝ่ายที่เกี่ยวข้องกับการเปลี่ยนแปลง (Drucker, 1995, อ้างถึงใน วิโรจน์ ก่อสกุล, 2568)

อย่างไรก็ตาม ข้อค้นพบที่น่าสนใจคือหน่วยงานมิได้นำหลักการการบริหารจัดการภาครัฐแนวใหม่มาใช้อย่างเต็มรูปแบบ หากแต่ปรับใช้ภายใต้เงื่อนไขด้านความมั่นคงเป็นสำคัญ ซึ่งหน่วยงานยังจำกัดการใช้งานระบบเฉพาะเอกสารทั่วไปและเอกสารเวียนเนื่องจากข้อกังวลเรื่องการรั่วไหลของข้อมูล และข้อมูลชั้นความลับสูงต้องแยกไปดำเนินการตามระเบียบว่าด้วยการรักษาความลับของทางราชการผ่านระบบเครือข่ายเฉพาะหรือเอกสาร

กระดาษเท่านั้น ข้อค้นพบดังกล่าวยืนยันข้อสังเกตของ Ferlie, Lynn, and Pollitt (2005) ที่ว่าการประยุกต์ใช้แนวคิดการบริหารจัดการภาครัฐแนวใหม่ในหน่วยงานด้านความมั่นคงมีความซับซ้อนเป็นพิเศษ เนื่องจากต้องสร้างสมดุลระหว่างความต้องการด้านประสิทธิภาพกับความต้องการด้านการรักษาความลับและการควบคุมการเข้าถึงระบบอย่างเข้มงวด

2. **ระบบบริหารจัดการสำนักงาน (e-Office) เสริมสร้างความโปร่งใสและความสามารถในการตรวจสอบตามหลักธรรมาภิบาล แต่ยังอยู่ในระยะเปลี่ยนผ่าน** ผลการวิจัยที่พบว่าผู้ส่งและผู้รับสามารถติดตามสถานะและเส้นทางของเอกสารได้แบบ Real-time ภายในระบบ ทำให้ทราบได้ว่าเรื่องที่เสนอไปอยู่ในขั้นตอนใดและผู้ใดเป็นผู้พิจารณา ซึ่งสะดวกกว่าระบบกระดาษที่ต้องเดินตามเรื่องเองนั้น สอดคล้องกับประโยชน์ของการนำหลักธรรมาภิบาลมาใช้ในการบริหารงาน ซึ่งช่วยให้หน่วยงานมีกลไกและกฎกติกาการบริหารจัดการที่เป็นระบบ มีความโปร่งใส และมีมาตรฐานการปฏิบัติงานที่ชัดเจน อันส่งผลให้องค์การได้รับความเชื่อถือและสามารถปรับตัวเท่าทันความเปลี่ยนแปลง (ทศพร ศิริสัมพันธ์, 2549, อ้างถึงใน วีณา พึงวิวัฒน์นิกุล, 2568) และสอดคล้องกับ Twizeyimana and Andersson (2019) ที่ชี้ว่ารัฐบาลอิเล็กทรอนิกส์ก่อให้เกิดคุณค่าสาธารณะทั้งด้านการเพิ่มประสิทธิภาพการบริหารจัดการและการเสริมสร้างความเชื่อมั่นในกระบวนการทำงานของภาครัฐ

อย่างไรก็ตาม เมื่อพิจารณาตามแบบจำลองวิวัฒนาการรัฐบาลอิเล็กทรอนิกส์ 4 ขั้นตอนของ Layne and Lee (2001) พบว่าการปฏิบัติราชการทางอิเล็กทรอนิกส์ของสำนักงานสภาความมั่นคงแห่งชาติยังอยู่ในช่วงคาบเกี่ยวระหว่างขั้นการทำธุรกรรม (Transaction) กับขั้นการบูรณาการแนวดิ่ง (Vertical Integration) เนื่องจากการส่งผ่านข้อมูลข้ามหน่วยงานยังเป็นลักษณะเอกสารแนบ ขาดการเชื่อมโยงในระดับชุดข้อมูล ประกอบกับยังมีกระบวนงานที่ต้องใช้เอกสารกระดาษควบคู่ จึงยังไม่บรรลุขั้นการบูรณาการแนวนอน (Horizontal Integration) ตามเป้าหมายของแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย

3. **กลไกธรรมาภิบาลข้อมูลของหน่วยงานมีความก้าวหน้ากว่าภาพรวมที่ปรากฏในผลสำรวจระดับความพร้อมรัฐบาลดิจิทัล** ผลการวิจัยที่พบว่าหน่วยงานได้จัดตั้งคณะกรรมการธรรมาภิบาลข้อมูลเป็นกลไกหลักในการกำกับดูแลการใช้ข้อมูลอย่างมีธรรมาภิบาล พร้อมทั้งออกนโยบายธรรมาภิบาลข้อมูลซึ่งระบุถึงการจัดหมวดหมู่และชั้นความลับของเอกสาร การบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล การพัฒนาข้อมูลให้มีคุณภาพ และการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล นับว่าครบถ้วนตามองค์ประกอบขั้นต่ำ 5 ประการที่บัญญัติไว้ในมาตรา 8 แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 และสอดคล้องกับกรอบธรรมาภิบาลข้อมูลภาครัฐของสำนักงานพัฒนารัฐบาลดิจิทัล (2566) ทั้งในมิติโครงสร้าง นิยามและกฎเกณฑ์ และกระบวนการตามวงจรการบริหารงานและพัฒนาคุณภาพงาน (PDCA)

ข้อค้นพบนี้นับว่ามีความก้าวหน้ากว่าภาพรวมของหน่วยงานภาครัฐไทย ซึ่งผลการสำรวจระดับความพร้อมรัฐบาลดิจิทัลพบว่าแม้หน่วยงานจะมีความตระหนักรู้เกี่ยวกับการจัดทำธรรมาภิบาลข้อมูลเพิ่มขึ้นอย่างต่อเนื่อง แต่จำนวนหน่วยงานที่ดำเนินการแล้วเสร็จและประกาศใช้ยังมีสัดส่วนค่อนข้างน้อย (สำนักงานพัฒนารัฐบาลดิจิทัล, 2565) ซึ่งอาจอธิบายได้ว่าสถานะการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านความมั่นคงของรัฐและลักษณะข้อมูลที่ส่วนใหญ่จัดอยู่ในหมวดข้อมูลความลับทางราชการและข้อมูลความมั่นคง เป็นแรงผลักดันเชิงบังคับให้หน่วยงานต้องวางกลไกกำกับดูแลข้อมูลที่เข้มข้นกว่าหน่วยงานทั่วไป อย่างไรก็ตาม มีข้อสังเกตเชิงวิเคราะห์ซึ่งชี้ว่าระบบ e-Office มิใช่กลไกการกำกับดูแลข้อมูลตามกรอบธรรมาภิบาลข้อมูลโดยตรง หากแต่เป็นเครื่องมือที่ช่วยสนับสนุนการดำเนินงานด้านธรรมาภิบาลข้อมูล

ทั้งการจัดเก็บเอกสารอย่างเป็นระบบ การสืบค้น การกำหนดสิทธิ์การเข้าถึงตามบทบาทหน้าที่ การตรวจสอบย้อนหลัง และการบริหารจัดการวงจรชีวิตข้อมูลนั้น ชี้ให้เห็นว่าการมีระบบสารสนเทศมิได้เท่ากับการมีธรรมาภิบาลข้อมูล หากแต่ต้องมีโครงสร้าง นโยบาย และกระบวนการกำกับดูแลรองรับควบคู่กันไป

4. **ความมั่นคงปลอดภัยไซเบอร์ในรูปแบบความรับผิดชอบร่วมเป็นลักษณะเฉพาะของการใช้ระบบกลางบนคลาวด์ภาครัฐ** ผลการวิจัยที่พบว่ามาตรการตามหน้าที่หลักทั้ง 5 ด้านของกรอบมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกรอบการรักษาความปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National institute of Standards and Technology: NIST) หรือ NIST Cybersecurity Framework มีลักษณะเป็นความรับผิดชอบร่วม (Shared Responsibility) ระหว่างเจ้าของระบบกับหน่วยงานผู้ใช้งาน โดยในมิติการระบุ (Identify) หน่วยงานจัดทำทะเบียนทรัพย์สินสารสนเทศเฉพาะส่วนอุปกรณ์ปลายทางและประเมินความเสี่ยงเฉพาะมิติความเสี่ยงจากการใช้งานของบุคลากรและช่องโหว่จากการเชื่อมต่อเครือข่ายภายใน ขณะที่ทรัพย์สินและสถาปัตยกรรมของระบบ e-Office และเครื่องแม่ข่ายหลักถูกระบุและประเมินความเสี่ยงโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและผู้ให้บริการคลาวด์กลางภาครัฐเป็นหลัก

ในทำนองเดียวกัน มิติการตรวจจับ (Detect) เป็นหน้าที่ของผู้ให้บริการคลาวด์ในระดับระบบปฏิบัติการและแอปพลิเคชัน ขณะที่หน่วยงานเฝ้าระวังในระดับเครือข่ายภายในและบันทึกการใช้งานของอุปกรณ์ปลายทาง ส่วนมิติการป้องกัน (Protect) หน่วยงานรับผิดชอบการยืนยันตัวตนผู้ใช้งานด้วยชื่อบัญชีและรหัสผ่าน การเชื่อมโยงกับระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล และอยู่ระหว่างการปรับเปลี่ยนไปสู่การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA)

นับเป็นข้อค้นพบที่สะท้อนบริบทเฉพาะของการใช้บริการคลาวด์กลางภาครัฐ (Cloud GDCC) กล่าวคือ เจ้าของระบบรับผิดชอบโครงสร้างพื้นฐาน การเข้ารหัสข้อมูล การสำรองข้อมูล และการเฝ้าระวังระดับแอปพลิเคชันภายใต้มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศหรือมาตรฐาน ISO/IEC 27001 ขณะที่หน่วยงานรับผิดชอบทะเบียนทรัพย์สินสารสนเทศของอุปกรณ์ปลายทาง การยืนยันตัวตน การกำหนดสิทธิ์การเฝ้าระวังเครือข่ายภายใน และการจัดทำแผนเผชิญเหตุ การจัดสรรความรับผิดชอบในลักษณะนี้สอดคล้องกับหลักการบริหารความเสี่ยง (Risk-based Approach) และวงจรการบริหารงานและพัฒนาคุณภาพงาน 4 ขั้นตอน ได้แก่ วางแผน (Plan) ปฏิบัติ (Do) ตรวจสอบ (Check) และ ปรับปรุง (Act) ของมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศหรือมาตรฐาน ISO/IEC 27001 ที่สามารถบูรณาการเข้ากับกรอบการรักษาความปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติได้ และสอดคล้องกับกรอบการประเมินระดับวุฒิภาวะด้านความมั่นคงปลอดภัยไซเบอร์ของ Bernardo, Malta, and Magalhães (2025) ที่เชื่อมโยงหน้าที่หลักทั้ง 5 ด้านเข้ากับการจัดลำดับความสำคัญของมาตรการควบคุมภายในองค์กร

5. **การบูรณาการกรอบธรรมาภิบาลข้อมูลกับกรอบความมั่นคงปลอดภัยไซเบอร์เป็นเงื่อนไขจำเป็นของหน่วยงานความมั่นคง** ผลการวิจัยแสดงให้เห็นว่าทั้งสองมิติมีความเกี่ยวเนื่องกันอย่างแยกไม่ออกในทางปฏิบัติ กล่าวคือ การจำแนกหมวดหมู่และการจัดชั้นความลับของข้อมูลตามกรอบธรรมาภิบาลข้อมูลเป็นพื้นฐานของการกำหนดมาตรการควบคุมการเข้าถึงและการเข้ารหัสตามกรอบความมั่นคงปลอดภัยไซเบอร์ และการกำหนดสิทธิ์ตามบทบาทหน้าที่ (Role-Based Access Control: RBAC) ก็เป็นทั้งกลไกธรรมาภิบาลข้อมูลและมาตรการป้องกัน (Protect) ตามกรอบ NIST ในเวลาเดียวกัน ข้อค้นพบนี้ช่วยเติมเต็มช่องว่างที่พบจากการทบทวนวรรณกรรมว่างานวิจัยส่วนใหญ่ทั้งในและต่างประเทศมักศึกษาสองมิตินี้แยกจากกัน (Alsaad, 2023) และสอดคล้องกับข้อเสนอเชิงนโยบายของ Keawwisut and Thongchana (2026) ที่เน้นการบริหารจัดการข้อมูลอย่างเป็นระบบควบคู่ไปกับการยกระดับความมั่นคงปลอดภัยไซเบอร์ในการพัฒนารัฐบาลดิจิทัลของประเทศไทย

จากผลการวิจัยตามวัตถุประสงค์ข้อ 2. นำมาอภิปรายได้ดังนี้

1. **ความเคยชินของบุคลากรและระดับการยอมรับเทคโนโลยีเป็นเงื่อนไขชี้ขาดความสำเร็จของระบบ** ผลการวิจัยที่พบว่าผู้ให้ข้อมูลสำคัญทุกคนระบุตรงกันว่าความเคยชินกับรูปแบบการทำงานเดิมเป็นอุปสรรคสำคัญที่สุดด้านบุคลากร จนก่อให้เกิดภาวะการทำงานซ้ำซ้อน กล่าวคือ การกรอกข้อมูลเข้าระบบพิมพ์ออกมาตรวจแก้ แล้วกรอกเข้าระบบใหม่นั้น ปรากฏการณ์ดังกล่าวสามารถอธิบายได้ด้วยทฤษฎีการยอมรับเทคโนโลยี (Technology Acceptance Model: TAM) ของ Davis (1989) และทฤษฎีรวมการยอมรับและการใช้เทคโนโลยี (UTAUT) ของ Venkatesh, Morris, Davis, and Davis (2003) กล่าวคือ ข้อค้นพบในระดับบริหารที่ระบุว่าการตรวจงานยังต้องพิมพ์เอกสารออกมาแก้ไขในบางครั้ง เนื่องจากการแก้ไขในระบบทำได้ยากและยังไม่คุ้นชินกับการใช้งาน สะท้อนถึงการรับรู้ความง่ายในการใช้งาน (Perceived Ease of Use) ที่อยู่ในระดับต่ำ ขณะที่ข้อมูลจากผู้ให้ข้อมูลอีกรายที่ระบุว่าเจ้าหน้าที่บางกลุ่มมองว่าการปฏิบัติงานผ่านระบบดิจิทัลมีความซับซ้อนและเข้าถึงยาก และเห็นว่าการเรียนรู้ทักษะดังกล่าวเป็นเรื่องไกลตัวหรือยังไม่จำเป็นเร่งด่วน จนขาดแรงจูงใจในการพัฒนาตนเอง สะท้อนถึงการรับรู้ประโยชน์ที่ได้รับ (Perceived Usefulness) ที่ยังไม่ชัดเจน

นอกจากนี้ ปัญหาความล่าช้าในการเข้าสู่ระบบ การแสดงผลค้าง และการที่ระบบไม่ตอบสนองในบางช่วงเวลา ยังสะท้อนเงื่อนไขสิ่งอำนวยความสะดวก (Facilitating Conditions) ตามกรอบทฤษฎีรวมการยอมรับและการใช้เทคโนโลยีที่ยังไม่เอื้อต่อการใช้งาน ข้อค้นพบทั้งหมดนี้สอดคล้องกับ Karnsomdee (2026) ที่พบว่าการสนับสนุนของผู้บริหาร แรงจูงใจ ความไว้วางใจ ความกังวลด้านความปลอดภัย และเงื่อนไขสิ่งอำนวยความสะดวกล้วนส่งผลอย่างมีนัยสำคัญต่อการยอมรับระบบภาครัฐ และสอดคล้องกับมานิตย์ กุศลคุ้ม (2562) ที่พบว่าด้านการรับรู้เป็นด้านที่บุคลากรมีความพร้อมน้อยที่สุดในการใช้ระบบสารบรรณอิเล็กทรอนิกส์

2. **ข้อจำกัดด้านเทคโนโลยีและทักษะบุคลากรเป็นข้อจำกัดร่วมของหน่วยงานภาครัฐไทย** ผลการวิจัยที่พบปัญหาความไม่เสถียรของระบบ ความล่าช้าในการประมวลผล ข้อจำกัดด้านฟังก์ชันและการบูรณาการข้อมูล ตลอดจนข้อจำกัดด้านทักษะดิจิทัลเชิงลึกของบุคลากร มีความสอดคล้องกับ Caplanova, Szakadatova, Tripathi, and Iqbal (2025) ที่พบว่าอุปสรรคสำคัญของการเปลี่ยนผ่านสู่ดิจิทัลของภาครัฐไทยอยู่ที่ทักษะดิจิทัลของบุคลากร การบูรณาการข้อมูล และความกังวลด้านความปลอดภัย และสอดคล้องกับจารุนันต์ เชาวนวาที และวงพักตร์ ภู่พันธ์ศรี (2567) ที่พบว่าการนำเทคโนโลยีดิจิทัลมาใช้ในหน่วยงานภาครัฐเผชิญอุปสรรคจากอุปกรณ์ที่ล้าสมัย บุคลากรที่ขาดความรู้ ทักษะ และความชำนาญ และความแตกต่างของช่วงอายุของเจ้าหน้าที่

นอกจากนี้ ประเด็นที่ควรให้ความสำคัญเป็นพิเศษคือความเสี่ยงจากองค์ความรู้ที่ผูกติดกับตัวบุคคล ซึ่งผลการวิจัยชี้ว่าหากเจ้าหน้าที่ผู้ดูแลระบบลาหรือพ้นจากองค์กรไป จะส่งผลให้องค์กรขาดผู้มีความรู้ความเชี่ยวชาญในระบบทันที ข้อค้นพบดังกล่าวสอดคล้องกับธนพงศ์ ฉันทวิเชียร (2566) ที่พบว่าอุปสรรคสำคัญของการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในหน่วยงานภาครัฐ ได้แก่ งบประมาณที่ไม่เพียงพอ บุคลากรขาดความรู้และทักษะ และจำนวนบุคลากรด้านไซเบอร์ที่มีจำกัด ซึ่งสะท้อนว่าปัญหาความเปราะบางด้านทุนมนุษย์มิได้เป็นปัญหาเฉพาะของหน่วยงานใดหน่วยงานหนึ่ง หากแต่เป็นปัญหาเชิงโครงสร้างของระบบราชการไทยในการเปลี่ยนผ่านสู่ดิจิทัล

3. **ความไม่เป็นเอกภาพของแนวปฏิบัติเกิดจากลักษณะยืดหยุ่นของระบบกลางประกอบกับการขาดแนวปฏิบัติมาตรฐานของหน่วยงาน** ผลการวิจัยที่พบว่าระบบกลางถูกออกแบบให้มีความยืดหยุ่นสูงเพื่อให้ทุกหน่วยงานใช้ร่วมกันได้ จนมีทางเลือกในการดำเนินการหลายวิธีสำหรับกระบวนการเดียวกัน ทำให้ทิศทางการใช้งานของแต่ละส่วนงานไม่เป็นไปในทิศทางเดียวกันนั้น ส่งผลกระทบชัดเจนในระดับผู้ปฏิบัติ โดยผู้ใช้งานสะท้อนว่าการที่แต่ละส่วนงานใช้งานระบบในรูปแบบที่แตกต่างกันก่อให้เกิดความสับสนในการประสานงานระหว่างส่วนงานโดยตรง ยิ่งไปกว่านั้น ยังพบพฤติกรรมการใช้ช่องว่างของระบบเพื่อให้

สามารถแสดงความเห็นบนเอกสารได้โดยไม่ต้องลงนาม ซึ่งเป็นวิธีที่ไม่ถูกต้องและก่อให้เกิดความเข้าใจกระบวนการทำงานของระบบที่ผิดวิธีในวงกว้าง ข้อค้นพบเหล่านี้สะท้อนช่องว่างเชิงกระบวนการซึ่งสอดคล้องกับเนตรชนก สุขสวัสดิ์ (2565) ที่เสนอว่าหน่วยงานส่วนกลางควรมีกลไกผลักดันโดยจัดตั้งทีมงานด้านเทคนิคสนับสนุนและกำหนดตัวชี้วัดความสำเร็จ เพื่อให้การนำระบบสารบรรณอิเล็กทรอนิกส์มาใช้เป็นไปในแนวทางเดียวกัน

นอกจากนี้ ผู้ให้ข้อมูลระดับนโยบายยังชี้ว่าเส้นทางการอนุมัติในระบบกลางมีรูปแบบที่ตายตัวเกินไป ไม่ยืดหยุ่นพอที่จะรองรับโครงสร้างการพิจารณากลั่นกรองเอกสารยุทธศาสตร์ความมั่นคงที่มีความเฉพาะตัวสูง ทำให้เจ้าหน้าที่ต้องสลับไปมาระหว่างกระบวนการทางอิเล็กทรอนิกส์สำหรับเอกสารทั่วไปกับกระบวนการดั้งเดิมสำหรับเอกสารลับ ส่งผลให้ภาพรวมของงานล่าช้า ซึ่งยืนยันข้อสังเกตของ Ferlie, Lynn, and Pollitt (2005) ที่ว่าหน่วยงานด้านความมั่นคงมีลักษณะเฉพาะที่ต้องการการปรับตัวเป็นพิเศษในการนำเครื่องมือการบริหารสมัยใหม่มาใช้

4. **โครงสร้างความรับผิดชอบร่วมบนระบบคลาวด์กลางเป็นทั้งโอกาสและความท้าทายเชิงธรรมาภิบาล** ผลการวิจัยที่พบความทับซ้อนของขอบเขตความรับผิดชอบระหว่างเจ้าของข้อมูล (Data Owner) กับผู้ประมวลผลข้อมูล (Data Processor) อันเนื่องมาจากระบบเป็นของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ที่ติดตั้งอยู่บนคลาวด์กลางภาครัฐ ขณะที่ข้อมูลเป็นของสำนักงานสภาความมั่นคงแห่งชาตินั้น สอดคล้องกับ Alsaad (2023) ที่ชี้ว่ากรอบธรรมาภิบาลข้อมูลจำนวนมากถูกพัฒนาจากมุมมองขององค์กรภาคธุรกิจ ขณะที่ธรรมาภิบาลข้อมูลภาครัฐมีขอบเขตเชิงองค์กรและวัตถุประสงค์การกำกับดูแลที่แตกต่างออกไป จึงจำเป็นต้องปรับโครงแบบของกรอบเดิมให้สอดคล้องกับบริบทเฉพาะของหน่วยงาน ข้อจำกัดดังกล่าวยังส่งผลต่อเนื่องถึงอำนาจในการจัดสรรงบประมาณเพื่อพัฒนาฟังก์ชันของระบบและความรวดเร็วในการเผชิญเหตุไซเบอร์ ซึ่งสะท้อนว่าการพึ่งพาโครงสร้างพื้นฐานของหน่วยงานภายนอกทำให้หน่วยงานสูญเสียอำนาจการควบคุมเชิงโครงสร้างไปในระดับหนึ่ง อันเป็นความเสี่ยงเชิงระบบที่มีนัยสำคัญเป็นพิเศษสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านความมั่นคงของรัฐ

จากผลการวิจัยตามวัตถุประสงค์ข้อ 3. นำมาอภิปรายได้ดังนี้

1. **บทบาทนำของผู้บริหารและแนวปฏิบัติมาตรฐานที่เป็นเอกภาพเป็นเงื่อนไขสำคัญของการขับเคลื่อน** ข้อเสนอแนะจากผู้ให้ข้อมูลสำคัญมีความสอดคล้องกันทั้งจากฝ่ายผู้ดูแลระบบและฝ่ายผู้ใช้งาน กล่าวคือ ฝ่ายผู้ใช้งานเสนอให้จัดทำคู่มือหรือแนวปฏิบัติมาตรฐาน (SOP) ที่ชัดเจน พร้อมการอบรมและประชาสัมพันธ์อย่างทั่วถึง เพื่อลดความสับสนและความคลาดเคลื่อนในการใช้งานและทำให้ทุกส่วนงานปฏิบัติงานไปในทิศทางเดียวกัน ขณะที่ฝ่ายผู้ดูแลระบบเน้นย้ำถึงบทบาทของผู้บริหารว่าการขับเคลื่อนควรเริ่มจากการสร้างแรงจูงใจและความตระหนักรู้ให้แก่เจ้าหน้าที่ ควบคู่กับการกำหนดนโยบายและแนวปฏิบัติที่มีความเป็นเอกภาพ ข้อเสนอดังกล่าวสอดคล้องอย่างยิ่งกับเนตรชนก สุขสวัสดิ์ (2565) ที่พบว่าการผลักดันจากผู้นำองค์กรเป็นเงื่อนไขสำคัญที่ส่งเสริมให้เกิดการใช้ระบบรับ-ส่งเอกสารผ่านระบบอิเล็กทรอนิกส์อย่างครบวงจร และสอดคล้องกับ Karnsomdee (2026) ที่ระบุว่าการสนับสนุนของผู้บริหารเป็นปัจจัยเชิงสถาบันที่มีอิทธิพลต่อการยอมรับระบบภาครัฐ ทั้งนี้ การกำกับให้มีการใช้งานครอบคลุมทั้งหน่วยงานยังต้องใช้เวลาปรับตัวและเผชิญแรงต้านตามธรรมชาติจากความคุ้นชินในวิถีการทำงานเดิม สะท้อนถึงความจำเป็นของการบริหารการเปลี่ยนแปลง (Change Management) ที่ต้องดำเนินควบคู่ไปกับการพัฒนาระบบเทคโนโลยี มิใช่การมุ่งพัฒนาเทคโนโลยีเพียงลำพัง

2. **การยกระดับธรรมาภิบาลข้อมูลจากการจัดเก็บเพื่อการสืบค้นสู่การใช้ข้อมูลเพื่อการวิเคราะห์เป็นการสร้างคุณค่าสาธารณะเพิ่มเติม** ให้เร่งรัดการจัดทำพจนานุกรมข้อมูล (Data Dictionary) และคำอธิบายชุดข้อมูลสำหรับเอกสารที่ผ่านการพิจารณาของผู้บริหารแล้ว เพื่อแปลงเอกสารที่จัดเก็บอยู่ในคลังให้กลายเป็น

ชุดข้อมูลที่มีโครงสร้าง (Structured Data) อันจะช่วยให้หน่วยงานสามารถนำข้อมูลเอกสารนโยบายไปใช้ประโยชน์ในการสืบค้นเชิงลึกและใช้เป็นฐานข้อมูลในการวิเคราะห์แนวโน้มยุทธศาสตร์ความมั่นคงในอนาคตนั้น สอดคล้องกับองค์ประกอบด้านการจัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐตามมาตรา 8 แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 และกรอบธรรมาภิบาลข้อมูลภาครัฐของสำนักงานพัฒนารัฐบาลดิจิทัล (2566) ทั้งยังสอดคล้องกับ Twizeyimana and Andersson (2019) ที่ชี้ว่าคุณค่าสาธารณะของรัฐบาลอิเล็กทรอนิกส์มิได้จำกัดอยู่เพียงการปรับปรุงบริการ แต่ครอบคลุมถึงการเพิ่มประสิทธิภาพการบริหารจัดการและการยกระดับความเชื่อมั่นในกระบวนการทำงาน อย่างไรก็ตาม ข้อเสนอให้ออกแบบระบบจัดการข้อมูลที่รองรับการประยุกต์ใช้ปัญญาประดิษฐ์จำเป็นต้องดำเนินควบคู่กับมาตรการคุ้มครองข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เนื่องจากข้อมูลในระบบประกอบด้วยทั้งข้อมูลอ่อนไหวและข้อมูลส่วนบุคคล

3. **การยกระดับมาตรการความมั่นคงปลอดภัยไซเบอร์ต้องดำเนินการทั้งในระดับเทคนิคและระดับการกำกับดูแลความสัมพันธ์กับเจ้าของระบบ** ในระดับเทคนิค พบว่าผู้ให้ข้อมูลสำคัญทุกระดับเสนอตรงกันให้เร่งรัดการบังคับใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) เพื่อป้องกันการเข้าสู่ระบบด้วยรหัสผ่านที่ถูกโจรกรรม ขณะที่ในระดับการกำกับดูแลความสัมพันธ์กับเจ้าของระบบ มีข้อเสนอให้ผลักดันการจัดทำขั้นตอนการปฏิบัติงานมาตรฐานร่วม (Joint SOP) ที่ระบุช่องทางการประสานงานฉุกเฉินตลอด 24 ชั่วโมง หรือการขอสิทธิ์ระดับผู้ดูแลระบบย่อย เพื่อให้เจ้าหน้าที่เทคนิคของหน่วยงานสามารถระงับบัญชีที่เกิดเหตุได้เองทันทีในกรณีวิกฤต

ข้อเสนอดังกล่าว รวมถึงข้อเสนอให้จัดทำข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) และการทดสอบเจาะระบบเชิงรุกในรูปแบบ Red Teaming Stress Test สอดคล้องกับปรมัตถ์ ไวรักษ์ (2562) ที่พบว่าบทบาทสำคัญของหน่วยงานกำกับดูแล คือ การวางกรอบแนวทางการรับมือภัยคุกคาม การกำหนดมาตรการและนโยบาย การตรวจสอบกำกับดูแล และการสร้างความร่วมมือเพื่อแบ่งปันข้อมูลข่าวสาร พร้อมทั้งเสนอแนะการฝึกซ้อมรับมือภัยคุกคามและการสร้างความตระหนักรู้เชิงรุก นอกจากนี้ การที่กรอบการรักษาความปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National institute of Standards and Technology: NIST) หรือ NIST Cybersecurity Framework ฉบับ 2.0 ได้เพิ่มหน้าที่หลักด้านการกำกับดูแลเข้ามา (National institute of Standards and Technology, 2024) ยังเป็นเครื่องยืนยันว่ามิติการกำกับดูแลความสัมพันธ์กับผู้ให้บริการภายนอกเป็นองค์ประกอบที่ขาดไม่ได้ของการบริหารความมั่นคงปลอดภัยไซเบอร์ร่วมสมัย ส่วนข้อเสนอเชิงมองการณ์ไกลในระดับนโยบายที่ให้สร้างระบบเข้ารหัสข้อมูลซึ่งสามารถต้านทานภัยคุกคามจากเทคโนโลยีควอนตัมนั้น สอดคล้องกับจีระวัฒน์ ลีนะกนิษฐ์ และทัธภร ธนาวริทธิ์ (2568) ที่ชี้ว่าประเทศไทยยังจำเป็นต้องยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ทั้งในเชิงนโยบาย โครงสร้างพื้นฐาน และบุคลากร ภายใต้บริบทสงครามลูกผสมที่การโจมตีทางไซเบอร์กลายเป็นเครื่องมือเชิงยุทธศาสตร์ และสะท้อนลักษณะเฉพาะของหน่วยงานความมั่นคงซึ่งข้อมูลมีมูลค่าเชิงความลับยาวนานกว่าหน่วยงานทั่วไป

4. **การพัฒนาสถาปัตยกรรมที่เป็นเอกเทศในระยะยาวเป็นการปรับกรอบมาตรฐานสากลให้สอดคล้องกับบริบทเฉพาะของหน่วยงานความมั่นคง** ข้อเสนอเชิงยุทธศาสตร์ที่สำคัญที่สุดประการหนึ่ง คือ การที่สำนักงานสภาความมั่นคงแห่งชาติในฐานะหน่วยงานความมั่นคงระดับนโยบายสูงสุด ควรพิจารณาศึกษาและพัฒนาระบบบริหารจัดการข้อมูลและการทำงานอิเล็กทรอนิกส์เป็นการภายใน (Secure Internal Work Platform) ที่มีมาตรฐานความปลอดภัยขั้นสูงสุด เนื่องจากในระยะยาวการพึ่งพาระบบ e-Office กลางสำหรับเอกสารทั่วไปเพียงอย่างเดียวอาจไม่ตอบโจทย์การยกระดับองค์กรสู่สำนักงานดิจิทัลอย่างเต็มรูปแบบ

ข้อเสนอดังกล่าวเป็นแนวทางที่ตอบสนองต่อข้อจำกัดเชิงโครงสร้างที่พบตามวัตถุประสงค์ข้อที่ 2 โดยตรง และสอดคล้องกับข้อเสนอของ Alsaad (2023) ที่ให้ปรับโครงแบบของกรอบธรรมาภิบาลข้อมูลเดิม โดยเพิ่มมิติขอบเขตเชิงองค์กรและขอบเขตเชิงข้อมูลให้สอดรับกับบริบทเฉพาะของหน่วยงาน ทั้งนี้ ผู้วิจัยเห็นว่า แนวทางดังกล่าวมิได้เป็นการปฏิเสธการใช้ระบบกลางของภาครัฐ หากแต่เป็นการจัดวางสถาปัตยกรรมแบบสองชั้น (Two-tier Architecture) กล่าวคือ ใช้ระบบกลางสำหรับเอกสารทั่วไปเพื่อประโยชน์ด้านการเชื่อมโยงระหว่างหน่วยงานตามนโยบายรัฐบาลดิจิทัล ควบคู่กับการมีระบบภายในที่ออกแบบให้มั่นคงปลอดภัยตั้งแต่ต้น (Secure by Design) สำหรับข้อมูลชั้นความลับ ซึ่งเป็นการสร้างสมดุลระหว่างประสิทธิภาพและความมั่นคงปลอดภัย

กล่าวโดยสรุป การอภิปรายผลข้างต้นชี้ให้เห็นว่า ความสำเร็จของการปฏิบัติราชการทางอิเล็กทรอนิกส์ของหน่วยงานด้านความมั่นคงมิได้ขึ้นอยู่กับความพร้อมของเทคโนโลยีเพียงลำพัง หากแต่เป็นผลจากปฏิสัมพันธ์ระหว่างปัจจัยด้านเทคโนโลยี ปัจจัยด้านบุคลากรและการยอมรับเทคโนโลยี ปัจจัยด้านกระบวนการ และปัจจัยด้านการกำกับดูแล โดยมีการบูรณาการกรอบธรรมาภิบาลข้อมูลเข้ากับกรอบความมั่นคงปลอดภัยไซเบอร์เป็นเงื่อนไขจำเป็นเฉพาะของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านความมั่นคงของรัฐ ซึ่งเป็นองค์ความรู้ที่งานวิจัยที่ผ่านมายังมิได้ศึกษาไว้อย่างเป็นระบบ

ข้อเสนอแนะ

ข้อเสนอแนะในการนำผลการวิจัยไปใช้ประโยชน์ ผู้วิจัยจัดลำดับตามระยะเวลาดำเนินการเป็น 3 ระยะ ดังนี้ ระยะสั้น สำนักงานสภาความมั่นคงแห่งชาติควรเร่งดำเนินการในสิ่งที่อยู่ในอำนาจของหน่วยงาน ได้แก่ จัดทำแนวปฏิบัติมาตรฐานและคู่มือการใช้งานที่ชัดเจนพร้อมจัดอบรมให้ทั่วถึงทุกส่วนงาน เร่งรัดการบังคับใช้การยืนยันตัวตนแบบหลายปัจจัย จัดตั้งทีมทบทวนและติดตามการใช้งานระบบเพื่อแก้ปัญหาองค์ความรู้ที่ผูกติดกับตัวบุคคล และสร้างแรงจูงใจแก่บุคลากรโดยผลักดันให้ผู้บริหารแสดงบทบาทนำในการใช้งานระบบ ระยะกลาง ควรประสานเจรจากับหน่วยงานภายนอก ได้แก่ เจรจากับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเพื่อปรับปรุงฟังก์ชันเปิดช่องทางเชื่อมต่อระหว่างกัน และพัฒนาการใช้งานบนอุปกรณ์เคลื่อนที่ จัดทำข้อตกลงระดับการให้บริการและขั้นตอนการปฏิบัติงานมาตรฐานร่วม และจัดทำบันทึกข้อตกลงความร่วมมือกับสำนักงานการตรวจเงินแผ่นดินเพื่อรองรับการตรวจสอบเอกสารทางการคลังแบบอิเล็กทรอนิกส์ และระยะยาว ควรเร่งรัดการจัดทำพจนานุกรมข้อมูลและคำอธิบายชุดข้อมูลหรือเมทาดาตา (Metadata) ออกแบบระบบจัดการข้อมูลรองรับปัญญาประดิษฐ์อย่างปลอดภัย เตรียมความพร้อมด้านการเข้ารหัสที่ต้านทานเทคโนโลยีควอนตัม และพิจารณาพัฒนาระบบทำงานอิเล็กทรอนิกส์ภายในที่มั่นคงปลอดภัยตามหลักการออกแบบที่มั่นคงปลอดภัยตั้งแต่ต้น (Secure by Design) สำหรับเอกสารชั้นความลับ

ข้อเสนอแนะสำหรับการวิจัย

ควรศึกษาเปรียบเทียบกับหน่วยงานด้านความมั่นคงอื่นหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในด้านอื่นเพื่อให้เห็นความเหมือนและความแตกต่างภายใต้บริบทที่หลากหลาย ควรใช้ระเบียบวิธีวิจัยเชิงปริมาณหรือแบบผสมโดยเก็บข้อมูลจากผู้ใช้งานในวงกว้างเพื่อวัดระดับการยอมรับเทคโนโลยีในเชิงสถิติ ควรศึกษาเชิงลึกเฉพาะประเด็นการพัฒนาสถาปัตยกรรมความมั่นคงปลอดภัยที่เป็นเอกเทศสำหรับข้อมูลชั้นความลับและการประยุกต์ใช้ปัญญาประดิษฐ์กับข้อมูลเอกสารนโยบายความมั่นคง ตลอดจนควรมีการศึกษาติดตามผลภายหลังจากที่หน่วยงานนำแนวทางการพัฒนาไปปฏิบัติ เพื่อประเมินประสิทธิผลของมาตรการและถอดบทเรียนสำหรับการพัฒนาอย่างต่อเนื่อง

เอกสารอ้างอิง

จารุนันต์ เชาวนวาที และวงพักตร์ ภู่พันธ์ศรี. (2567). *การนำเทคโนโลยีดิจิทัลมาใช้ในการสนับสนุนงานตรวจราชการ: กรณีศึกษา กองตรวจราชการ สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม*. วารสารรามคำแหง ฉบับรัฐประศาสนศาสตร์, 7(2), 418–450.

จีระวัฒน์ ลีนะกนิษฐ์ และทัธภร ธนาวริทธิ์. (2568). *การพัฒนาศักยภาพความมั่นคงทางไซเบอร์: ศึกษาบริบทสงครามลูกผสมในประเด็นความท้าทายและการรับมือของประเทศไทย*. วารสารศิลปการจัดการ, 9(4).

ธนพงศ์ ฉันทวิเชียร. (2566). *การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9*. สารนิพนธ์รัฐประศาสนศาสตรมหาบัณฑิต, มหาวิทยาลัยสงขลานครินทร์. คลังปัญญามหาวิทยาลัยสงขลานครินทร์.

เนตรชนก สุขสวัสดิ์. (2565). *แนวทางการส่งเสริมสำนักงานจังหวัดนำระบบสารบรรณอิเล็กทรอนิกส์ (e-Saraban) ของสำนักงานปลัดกระทรวงมหาดไทยมาใช้ให้เป็นแนวทางเดียวกัน* (สารนิพนธ์รัฐประศาสนศาสตรมหาบัณฑิต). กรุงเทพมหานคร: จุฬาลงกรณ์มหาวิทยาลัย.

ปรมัตถ์ ไวรักษ์. (2562). *การศึกษามาตรการความมั่นคงปลอดภัยทางไซเบอร์ต่อสถาบันการเงิน วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต*, จุฬาลงกรณ์มหาวิทยาลัย. Chula Digital Collections.

ปะการัง ชื่นจิต. (2568). *เอกสารประกอบการบรรยายกระบวนวิชาขอบข่ายและแนวคิดเชิงทฤษฎีรัฐประศาสนศาสตร์.* กรุงเทพมหานคร: มหาวิทยาลัยรามคำแหง, โครงการรัฐประศาสนศาสตรมหาบัณฑิต.

มานิตย์ กุศลคุ้ม. (2562). *ความพร้อมต่อการใช้ระบบสารบรรณอิเล็กทรอนิกส์ของบุคลากรมหาวิทยาลัยราชภัฏธนบุรี.* กรุงเทพมหานคร: มหาวิทยาลัยราชภัฏธนบุรี.

วิโรจน์ ก่อสกุล. (2568). *เอกสารประกอบการบรรยายกระบวนวิชาองค์การและนวัตกรรมในองค์การ.* กรุงเทพมหานคร: มหาวิทยาลัยรามคำแหง, โครงการรัฐประศาสนศาสตรมหาบัณฑิต.

วีณา พึงวิวัฒน์นิกุล. (2568). *เอกสารประกอบการบรรยายกระบวนวิชาการจัดการทรัพยากรมนุษย์ร่วมสมัย.* กรุงเทพมหานคร: มหาวิทยาลัยรามคำแหง, โครงการรัฐประศาสนศาสตรมหาบัณฑิต.

สำนักงานพัฒนารัฐบาลดิจิทัล. (2566). มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ (ฉบับปรับปรุง: แนวปฏิบัติ) (มรด. 6: 2566). กรุงเทพมหานคร: สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน).

สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. (2561). ยุทธศาสตร์ชาติ (พ.ศ. 2561–2580). กรุงเทพมหานคร: สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ.

Alsaad, A. (2023). *Governmental data governance frameworks: A systematic literature review. In Proceedings of the 2023 International Conference on Computing, Electronics & Communications Engineering (iCCECE)* (pp. 150–156). IEEE. Retrieved May 20, 2026 from https://doi.org/10.1109/iCCECE59400.2023.10238504

Bernardo, L., Malta, S., & Magalhães, J. (2025). An evaluation framework for cybersecurity maturity aligned with the NIST CSF. Electronics, 14(7), 1364. Retrieved May 20, 2026 https://doi.org/10.3390/electronics14071364

Caplanova, A., Szakadatova, E., Tripathi, D., & Iqbal, A. (2025). *Digitalisation of the public sector in Thailand – Insights into Thailand's public sector digitalisation strategy*. Open Research Europe, 5, 209. Retrieved May 21, 2026 https://doi.org/10.12688/openreseurope.19868.1

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. Retrieved May 21, 2026 https://doi.org/10.2307/249008

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). New public management is dead—Long live digital-era governance. *Journal of Public Administration Research and Theory*, 16(3), 467–494. Retrieved May 22, 2026 https://doi.org/10.1093/jopart/mui057

Ferlie, E., Lynn, L. E., Jr., & Pollitt, C. (Eds.). (2005). *The Oxford handbook of public management*. Oxford: Oxford University Press.

Karnsomdee, P. (2026). Institutional determinants of smart government adoption: Evidence from Thai public sector organizations. *Frontiers in Political Science.* Retrieved May 20, 2026 https://doi.org/10.3389/fpos.2026.1732138

Keawwisut, S., & Thongchana, P. (2026). Digital government and the transformation of Thailand's public sector: Trends and challenges. *Princess of Naradhiwas University Journal of Humanities and Social Sciences, 13*(1), 284–301.

Layne, K., & Lee, J. (2001). Developing fully functional e-government: A four stage model. *Government Information Quarterly, 18*(2), 122–136. Retrieved May 24, 2026 https://doi.org/10.1016/S0740-624X(01)00066-1

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1).* Washington, DC: U.S. Department of Commerce. Retrieved May 22, 2026 https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29).* Washington, DC: U.S. Department of Commerce. Retrieved May 25, 2026 https://doi.org/10.6028/NIST.CSWP.29

Twizeyimana, J. D., & Andersson, A. (2019). The public value of e-government – A literature review. *Government Information Quarterly, 36*(2), 167–178. Retrieved May 26, 2026 https://doi.org/10.1016/j.giq.2019.01.001

United Nations. (2022). *E-Government Survey 2022*: The future of digital government. New York, NY: Department of Economic and Social Affairs, United Nations.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478. Retrieved May 23, 2026 https://doi.org/10.2307/30036540

ผู้ให้ข้อมูลสำคัญ

ผู้ให้ข้อมูลสำคัญคนที่ 1. (2569) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร. สัมภาษณ์ส่วนบุคคล. กรกฎาคม, 2

ผู้ให้ข้อมูลสำคัญคนที่ 2. (2569) เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร. สัมภาษณ์ส่วนบุคคล. กรกฎาคม, 1

ผู้ให้ข้อมูลสำคัญคนที่ 3. (2569) นักวิชาการคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร. สัมภาษณ์ส่วนบุคคล. กรกฎาคม, 1

ผู้ให้ข้อมูลสำคัญคนที่ 4. (2569) เจ้าหน้าที่วิเคราะห์นโยบายและแผน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร. สัมภาษณ์ส่วนบุคคล. กรกฎาคม, 2

ผู้ให้ข้อมูลสำคัญคนที่ 5. (2569) นักวิเคราะห์นโยบายและแผน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร. สัมภาษณ์ส่วนบุคคล. กรกฎาคม, 3