ศูนย์สารสนเทศและการสื่อสาร
สบอ. ๙ (อุบลราชธานี)
เลขที่รับ 10019
วันที่ 10 ก.ย. 69

บันทึกข้อความ

ส่วนราชการ สำนักบริหารพื้นที่อนุรักษ์ที่ ๙ (อุบลราชธานี) ส่วนอำนวยการ โทร ๐ ๔๕๓๑ ๑๖๗๗ ต่อ ๑๐๗
ที่ ทส ๐๙๑๙.๑๐๒/๕๐๑๓๓ **วันที่** ๙ กันยายน ๒๕๖๙
เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi – Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย

เรียน ผู้อำนวยการส่วนทุกส่วน
หัวหน้าศูนย์ทุกศูนย์

สำนักบริหารพื้นที่อนุรักษ์ที่ ๙ (อุบลราชธานี) ขอส่งสำเนาหนังสือกองแผนงานและสารสนเทศ ที่ ทส ๐๙๐๕.๒๐๔/ว ๔๐๐๘๑ ลงวันที่ ๘ กันยายน ๒๕๖๙ เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหลด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi – Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย มาเพื่อทราบและพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

(นายนิวัฒน์ สงมา)
เจ้าพนักงานป่าไม้อาวุโส รักษาราชการแทน
ผู้อำนวยการสำนักบริหารพื้นที่อนุรักษ์ที่ ๙

เรียน หัวหน้าศูนย์สารสนเทศ
-เห็นควรเผยแพร่ในเว็บ สบอ. ๙ อุบล
ทางเพจ สบอ. ๙ อุบล Noon. com.
-เรียนมาเพื่อทราบ

นางเจริญพร จิรมงคลการ
พนักงานธุรการ ส ๓

ทราบ
ดำเนินการตามเสนอ

(นายณฐพร ศรีพรหม)
นักวิชาการป่าไม้ชำนาญการ
หัวหน้าศูนย์สารสนเทศและการสื่อสาร

...ายยุทธศาสตร์และแผน
เลขรับ 10041
รับที่ - 8 ก.ย. 2569
เวลา 13:29 น.

สำนักบริหารพื้นที่อนุรักษ์ที่ ๙
เลขรับ 4915
วันที่ 8 ก.ย. 2569

บันทึกข้อความ

ส่วนราชการ กองแผนงานและสารสนเทศ ส่วนนโยบายและแผน โทร. ๐ ๒๕๖๓ ๐๗๗๗ ต่อ ๑๒๓๓

ที่ ทส ๐๙๐๕.๒๐๔/ว ๒๐๐๔๑ **วันที่** ๔ กันยายน ๒๕๖๙

เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย

สำนักอำนวยการ
เลขที่รับ ๔๐๐๔๘
วันที่รับ 8 ก.ย. 2569
เวลา

หน้าห้อง ผอ. สบอ.9
เลขที่รับ 4002
วันที่/เวลา 9 ก.ย. 2569
ส่งคืน/แก้ไข
รับคืน

เรียน รองอธิบดีกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ทุกท่าน
ผู้ตรวจราชการกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ทุกท่าน
เลขานุการกรม
ผู้อำนวยการกองทุกกอง
ผู้อำนวยการสำนักบริหารพื้นที่อนุรักษ์ที่ ๑-๑๖
ผู้เชี่ยวชาญเฉพาะด้านการอนุรักษ์ทรัพยากรป่าไม้และสัตว์ป่า
หัวหน้ากลุ่มงานจริยธรรม
ผู้อำนวยการสำนักสนองงานพระราชดำริ
ผู้อำนวยการสำนักบริหารพื้นที่อนุรักษ์สาขาทุกสาขา
ผู้อำนวยการสำนักงานผู้ตรวจราชการกรม
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ผู้อำนวยการศูนย์ควบคุมมาตรฐานการลาดตระเวนเชิงคุณภาพ (SMART PATROL)
ผู้อำนวยการกลุ่มตรวจสอบภายใน
ผู้อำนวยการกลุ่มพัฒนาระบบบริหาร
ผู้อำนวยการศูนย์ราชการสะดวก กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช
ผู้อำนวยการศูนย์ข่าวกรองอาชญากรรมสัตว์ป่า (WILDLIFE CRIME INTELLIGENCE CENTER)
ผู้อำนวยการสำนักงานโครงการป่าไม้เพื่อชีวิตฯ

กองแผนงานและสารสนเทศ ขอส่งสำเนาหนังสือสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม ที่ ทส ๐๒๐๗.๔/ว ๓๐๐๔ ลงวันที่ ๓๓ สิงหาคม ๒๕๖๙ พร้อมสำเนาหนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๕/ว ๖๙๖ ลงวันที่ ๑๔ สิงหาคม ๒๕๖๙ เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi – Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ในการนี้ นายนวินทร์ ประทวนชัย รองอธิบดี รักษาราชการแทนอธิบดีกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ได้โปรดมีบันทึกสั่งการท้ายหนังสือดังกล่าว เมื่อวันที่ ๓ กันยายน ๒๕๖๙ ความว่า "มอบ กผส./ศทส. พิจารณา" มาเรียนเพื่อโปรดทราบและพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป รายละเอียดปรากฏตาม QR Code ท้ายหนังสือที่แนบมาพร้อมนี้

☑ สธก. ☐ สอช. ☐ กกม.
☐ สตท. ☐ สอป. ☐ ศทส.
☐ สทป. ☐ สจท. ☐ สนช.
☐ สทอ. ☐ สวช. ☐ สนอ.
☐ ศทส.

(นายนิวัฒน์ สงมา)
ผู้อำนวยการส่วนอำนวยการ

(นายมานัส ปานขม)
ผู้อำนวยการกองแผนงานและสารสนเทศ

ที่ ทส ๐๒๐๗.๔/ว ๓๐๐๕ วันที่ ๒๓ ส.ค. ๒๕๖๙

เรียน อธิบดี ทุกกรม ปธ
เลขาธิการ สผ.
ผอ.รัฐวิสาหกิจ ทุกแห่ง
ผอ.องค์การมหาชน ทุกแห่ง

เพื่อโปรดทราบและพิจารณาดำเนินการ

ทั้งนี้ สามารถดาวน์โหลดเอกสารข้อมูลได้จาก QR Code ที่ปรากฏท้ายหนังสือฉบับนี้

(นายนิพนธ์ จำนงสิริศักดิ์)
รองปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม
ปฏิบัติราชการแทนปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม
27 ส.ค. 2569

รอง ปกท.ทส. (นายนิพนธ์ จำนงสิริศักดิ์)
หัวหน้ากลุ่มภารกิจด้านทรัพยากรธรรมชาติ
เลขรับ 6155
วันที่ 27 ส.ค. 2569
เวลา 11.55 น.

รอง ปกท.ทส. (นายประเสริฐ ศรีมงกุฎ)
เลขรับ 9106
วันที่ 27 ส.ค. 2569
เวลา 11:40 น.

ที่ ทส ๐๒๐๗.๔/ว๓๐๐๕ วันที่ ๒๖ ส.ค. ๒๕๖๙

เรียน ปกท.ทส.

เพื่อโปรดพิจารณาลงนาม

(นางสาววิสุตรา รัตนโสภา)
ผู้อำนวยการกองยุทธศาสตร์และแผนงาน

https://shorturl.at/INHdJ
นร ๐๕๐๕/ว ๒๙๖
สป.ทส. (กยผ.) อมรรัตน์
โทร. ๐ ๒๒๖๕ ๒๔๖๑

สำนักงานปลัดกระทรวง
ทรัพยากรธรรมชาติและสิ่งแวดล้อม
เลขรับ 18956
วันที่ ๒๘ ส.ค. ๒๕๖๙
เวลา 10:24 น.

ส่วนนโยบายและแผน
รับที่ 40064
วันที่ 7 ก.ย. 2569
เวลา 09.05 น.

ฝ่ายประสานงานคณะรัฐมนตรีฯ
รับที่ 21
วันที่ 7 ก.ย. 2569
เวลา 09.15 น.

สำนักงานปลัดกระทรวง
ทรัพยากรธรรมชาติและสิ่งแวดล้อม
เลขรับ 60328
วันที่ 7 ก.ย. 2569
เวลา 10.27

ห้อง อสส.
เลขที่รับ 40094
วันที่ 7 ก.ย. 2569
เวลา 11.28 น.

ห้องรอง อสส.
(นายนริทร์ ประหวนชัย)
เลขที่รับ 40091
วันที่ 7 ก.ย. 2569
เวลา 14:50 น.

กองแผนงานและสารสนเทศ
เลขรับ 40243
วันที่ 9 ก.ย. 69
เวลา 13.30 น.

-ลอย กสส./ศูนย์. ฟังบน.

(นายนริทร์ ประหวนชัย)
รองอธิบดี รักษาราชการแทน
อธิบดีกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

เรียน ผอ.ส่วนนโยบายและแผน
โปรดพิจารณาดำเนินการต่อไป

(นางสมหญิง ดวงสถาพร)
ผู้เชี่ยวชาญด้านนโยบายและแผน
รักษาราชการแทนผู้อำนวยการกองแผนงานและสารสนเทศ

ฝ่ายประสานงานคณะรัฐมนตรีฯ
พิจารณาดำเนินการ
7/ก.ย.69

(นางพรรณวิภา เจริญชนโชติ)
ผู้อำนวยการส่วนนโยบายและแผน
-ทราบ

เลขรับ ๕๒๑๐
วันที่ ๒๑ ส.ค. ๒๕๖๙
เวลา ๑๖.๔๐

ที่ดับ ๑๑๘๗



ทส. รับที่ 18336 วันที่ 20 ส.ค. 2569 เวลา 16.02

สำนักราชรัฐมนตรี ทส. รับที่ 3624 วันที่ 27 ส.ค. ๒๕๖๙ เวลา 09.39 น.

ด่วนที่สุด

ที่ นร ๐๕๐๕/ว ๒๙๖

สำนักเลขาธิการคณะรัฐมนตรี
ทำเนียบรัฐบาล กทม. ๑๐๓๐๐

๑๔ สิงหาคม ๒๕๖๙

ห้อง ปกท.ทส.
เลขรับ 5742
วันที่ ๒๑ ส.ค. ๒๕๖๙
เวลา 8.41 น.

ส่วน ปคร.
รับที่ 2015 เวลา 16.06 น.
วันที่ ๒๔ ส.ค. ๒๕๖๙

เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย

เรียน รัฐมนตรีว่าการกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

สิ่งที่ส่งมาด้วย บัญชีสำเนาหนังสือที่ส่งมาด้วย

ด้วยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้เสนอเรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ไปเพื่อดำเนินการ ซึ่งหน่วยงานที่เกี่ยวข้องได้เสนอความเห็นไปเพื่อประกอบการพิจารณาของคณะรัฐมนตรีด้วย ความละเอียดปรากฏตามบัญชีสำเนาหนังสือที่ส่งมาด้วยนี้

ในคราวประชุมคณะรัฐมนตรีเมื่อวันที่ ๑๑ สิงหาคม ๒๕๖๙ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเสนอเพิ่มเติมว่า ปัจจุบันมีการรั่วไหลของข้อมูลในภาคราชการเป็นจำนวนมาก ซึ่งรวมถึงข้อมูลและรหัสผ่านสำหรับเข้าใช้ระบบของหน่วยงานของรัฐ โดยข้อมูลหลายชุดเป็นบัญชีผู้ใช้งานระดับผู้ดูแลระบบ ดังนั้น จึงเห็นควรให้หน่วยงานของรัฐดำเนินการเพื่อป้องกันและแก้ไขปัญหาการรั่วไหลของข้อมูลดังกล่าว ดังนี้

๑. ให้หน่วยงานของรัฐทุกแห่งตั้งรหัสผ่านใหม่ (Reset Password) สำหรับบัญชีผู้ใช้งานระบบสารสนเทศทั้งหมด พร้อมทั้งปรับเปลี่ยนไปใช้ระบบการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication: MFA) เพื่อยกระดับความปลอดภัยและป้องกันการเข้าถึงระบบให้มีประสิทธิภาพมากยิ่งขึ้น

๒. ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หารือร่วมกับหน่วยงานอื่นที่เกี่ยวข้องเพื่อจัดทำแนวทางในการตรวจสอบระบบข้อมูลของหน่วยงานของรัฐ ทั้งระบบที่ใช้งานอยู่ในปัจจุบันและระบบที่เลิกใช้งานแล้ว เพื่อปรับปรุงระบบข้อมูลดังกล่าวให้ถูกต้องและเป็นปัจจุบัน (Data Cleansing) โดยเร็วต่อไป

/ซึ่งคณะรัฐมนตรี ...

ซึ่งคณะรัฐมนตรีพิจารณาแล้วลงมติว่า

๑. เห็นชอบและอนุมัติตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอและที่รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเสนอเพิ่มเติม

๒. ให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) และหน่วยงานอื่นที่เกี่ยวข้องรับความเห็นของกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม กระทรวงสาธารณสุข สำนักงบประมาณ สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ และสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ไปพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

จึงเรียนยืนยันมา และขอได้โปรดดำเนินการตามมติคณะรัฐมนตรีในส่วนที่เกี่ยวข้องต่อไป

เรียน ผบ. ทสน. และ ผบ. ชอ.

☑ เพื่อพิจารณาดำเนินการ
☐ มอบหมายเป็นผู้แทน
☐ เพื่อทราบ
☐ .....

ขอแสดงความนับถือ

(นางณัฐฏ์จารี อนันตศิลป์)
เลขาธิการคณะรัฐมนตรี

(นางรวีวรรณ ภูริเดช)
ปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม
๒๑ ส.ค. ๒๕๖๙

ที่ นร 0100/ว ๑๑๗ ๒๐ ส.ค. 2569

เรียน ปกท.ทส.
รมว.ทส. มีบัญชามอบ ปกท.ทส.
ดำเนินการต่อไป

พล.ต.ต.
(สุรพล บุญมา)
เลขานุการ รมว.ทส.

เรียน ☐ นรช.ด้านนโยบายและยุทธศาสตร์.....
☐ ผอ.สอก. .....
☐ ผอ.สนร. .....
☐ ผอ.สผค. .....
☐ ผอ.สงป. .....
☐ ผอ.สปส. .....
☑ ผอ.สปคร. .....

(นางสาวพิสุตรา รัตนโสภา)
ผู้อำนวยการกองยุทธศาสตร์และแผนงาน

กองพัฒนายุทธศาสตร์และติดตามนโยบายพิเศษ
โทร. ๐ ๒๒๘๐ ๙๐๐๐ ต่อ ๑๖๓๒ (วีนัสรินทร์), ๑๕๐๙ (สมจิตร)
โทรสาร ๐ ๒๒๘๐ ๑๔๔๖
www.soc.go.th
ไปรษณีย์อิเล็กทรอนิกส์ saraban@soc.go.th

บัญชีสำเนาหนังสือที่ส่งมาด้วย

เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย

๑. สำเนาหนังสือคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ด่วนที่สุด ที่ สกมช ๐๔๑๐/๒๔๗๓ ลงวันที่ ๒๑ กรกฎาคม ๒๕๖๙

๒. สำเนาหนังสือกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ด่วนที่สุด ที่ อว (ปคร) ๐๒๓๓/๑๖๕๒๓ ลงวันที่ ๑๓ สิงหาคม ๒๕๖๙

๓. สำเนาหนังสือกระทรวงคมนาคม ด่วนที่สุด ที่ คค (ปคร) ๐๒๑๐/๒๖๑ ลงวันที่ ๑๓ สิงหาคม ๒๕๖๙

๔. สำเนาหนังสือกระทรวงสาธารณสุข ที่ สธ ๐๒๑๒/๖๔๗๙ ลงวันที่ ๗ สิงหาคม ๒๕๖๙

๕. สำเนาหนังสือสำนักงบประมาณ ด่วนที่สุด ที่ นร ๐๙๐๔/๕๑๖ ลงวันที่ ๑๐ สิงหาคม ๒๕๖๙

๖. สำเนาหนังสือสำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ ด่วนที่สุด ที่ นร ๑๑๑๖/๓๔๑๓ ลงวันที่ ๑๑ สิงหาคม ๒๕๖๙

๗. สำเนาหนังสือสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ด่วน ที่ สพร ๒๕๖๑/๑๓๗๕ ลงวันที่ ๑๐ สิงหาคม ๒๕๖๙

NCS
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ หมู่ ๓ อาคารซี ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

ด่วนที่สุด
ที่ สกมช ๐๘๑๐/ห ๘๗๑

๒๑ กรกฎาคม ๒๕๖๙

เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย

เรียน เลขาธิการคณะรัฐมนตรี

สิ่งที่ส่งมาด้วย ๑. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ จำนวน ๑ ฉบับ
๒. (สำเนา) รายงานการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๑/๒๕๖๙
๓. (สำเนา) คำสั่งสำนักนายกรัฐมนตรี ที่ ๙๖/๒๕๖๙ ลงวันที่ ๒๙ เมษายน ๒๕๖๙ จำนวน ๑ ฉบับ
๔. (สำเนา) คำสั่งสำนักนายกรัฐมนตรี ที่ ๙๒/๒๕๖๙ ลงวันที่ ๗ เมษายน ๒๕๖๙ จำนวน ๑ ฉบับ

ด้วย คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ขอเสนอเรื่องแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย มาเพื่อคณะรัฐมนตรีพิจารณา โดยเรื่องนี้เข้าข่ายที่จะให้นำเสนอคณะรัฐมนตรีได้ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๐) และพระราชกฤษฎีกาว่าด้วยการเสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๙ (๑) และมาตรา ๖ (๑) ทั้งนี้ รัฐมนตรีประจำสำนักนายกรัฐมนตรี (นายภราดร ปริศนานันทกุล) ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ได้เห็นชอบให้นำเรื่องดังกล่าวเสนอคณะรัฐมนตรี ด้วยแล้ว

ทั้งนี้ เรื่องดังกล่าวมีรายละเอียด ดังนี้

๑. <u>เหตุผลความจำเป็นที่ต้องเสนอคณะรัฐมนตรี</u>

การเสนอกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล มีความจำเป็นต้องเสนอคณะรัฐมนตรีเพื่อพิจารณาและให้ความเห็นชอบ เนื่องจากเป็นการดำเนินการตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๐) ซึ่งกำหนดให้ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่เสนอแนะและให้ความเห็นต่อคณะรัฐมนตรีเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ดังนั้น เรื่องนี้จึงเข้าข่ายเรื่องที่ต้องเสนอคณะรัฐมนตรีตาม พระราชกฤษฎีกาว่าด้วยการเสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๙ (๑) เรื่องที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของคณะรัฐมนตรีหรือให้ต้องเสนอคณะรัฐมนตรี และมาตรา ๖ (๑) ในกรณีที่คณะกรรมการใดมีนายกรัฐมนตรี รองนายกรัฐมนตรี หรือรัฐมนตรีประจำสำนักนายกรัฐมนตรี รัฐมนตรีว่าการกระทรวงหรือทบวงเป็นประธานกรรมการของคณะกรรมการนั้นให้นายกรัฐมนตรี รองนายกรัฐมนตรี รัฐมนตรีประจำสำนักนายกรัฐมนตรี รัฐมนตรีว่าการกระทรวงหรือทบวง แล้วแต่กรณีในฐานะประธานกรรมการเป็นผู้ลงนามเสนอเรื่องต่อคณะรัฐมนตรีได้

๒. ความเร่งด่วนของเรื่อง

ด้วยเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานต่าง ๆ ภายในประเทศ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) หรือ ThaiCERT ได้ดำเนินการเฝ้าระวัง ตรวจสอบ และได้ร่วมเผชิญเหตุตอบสนองรับมือกับภัยคุกคามที่เกิดขึ้นหลายเหตุการณ์ พบว่าสาเหตุหลักที่หน่วยงานถูกโจมตีและส่งผลกระทบต่อการให้บริการภาคประชาชนหยุดชะงัก คือผู้โจมตีได้รับข้อมูลบัญชีผู้ใช้งาน (Credential) สำหรับการยืนยันตัวตนจากแหล่ง ซื้อขาย เช่น Dark Web และ Breach Forum รวมถึงมีการแชร์ข้อมูลบัญชีผู้ใช้งาน (Credential) ที่ขโมยมาได้ในกลุ่ม Telegram โดยผู้โจมตีจะใช้ข้อมูลที่ได้มาในการเข้าถึงช่องทางเครือข่ายภายในของหน่วยงาน อย่างเช่น ระบบ VPN และใช้ข้อมูลเหล่านั้นเข้าสู่ระบบงานสำคัญต่าง ๆ จากนั้นก็ทำการขโมยข้อมูลของหน่วยงานออกไปและโจมตีเพื่อทำลายระบบต่าง ๆ ด้วย ransomware เป็นต้น

เพื่อให้เป็นการยกระดับการป้องกันไม่ให้หน่วยงานต่าง ๆ ที่อาจมีข้อมูลบัญชีผู้ใช้งาน (Credential) ถูกขโมยหรือรั่วไหล และทำให้ Hacker สามารถเข้าถึงระบบงานต่าง ๆ ของหน่วยงาน และเป็นสาเหตุให้ข้อมูลส่วนบุคคลหลุดรั่ว ตลอดจนโจมตีหน่วยงานเพื่อขโมยข้อมูลหรือเข้ารหัสข้อมูลส่งผลกระทบต่อการดำเนินงานหรือระบบงานต่าง ๆ และอาจจะส่งผลกระทบต่อระบบบริการต่าง ๆ ที่ให้บริการแก่ประชาชนได้ สกมช. จึงขอเสนอแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ต่อคณะรัฐมนตรีพิจารณาให้หน่วยงานดำเนินการตามแนวทางดังกล่าวต่อไป

๓. สาระสำคัญและข้อเท็จจริง

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ได้มีการจัดประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ครั้งที่ ๑/๒๕๖๙ เมื่อวันที่ ๒๕ พฤษภาคม ๒๕๖๙ โดยมีระเบียบวาระที่ ๔.๕ เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) ได้ดำเนินการติดตามวิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ รวมถึงการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ศปช. ได้ดำเนินการได้ทำการสืบสวนสอบสวนและตรวจพิสูจน์จนพบว่ากลุ่มผู้ไม่หวังดีใช้ชื่อว่า ALIEN TXTBASE Stealer Logs ซึ่งเป็นกลุ่มที่มีพฤติกรรมในการละเมิดและขโมยข้อมูลบัญชีผู้ใช้งาน จากนั้นได้มีการแชร์ข้อมูลที่ขโมยมาได้ในกลุ่ม Telegram ที่รู้จักกันในชื่อ ALIEN TXTBASE ซึ่งชุดข้อมูลที่แชร์มีจำนวนมากกว่า ๑๖,๕๒๐ ไฟล์ ขนาดของไฟล์รวมกัน มีขนาดมากกว่า 5TB และได้มีการแชร์อัปเดตชุดข้อมูลในทุกวัน ซึ่งข้อมูลนี้ประกอบด้วยที่อยู่อีเมลเฉพาะตัว จำนวนหลายล้านรายการ พร้อมทั้งเว็บไซต์ที่เข้าใช้ระบบงานของหน่วยงานจำนวนมากและรหัสผ่านที่ใช้ โดยหลายชุดข้อมูลเป็นบัญชีผู้ใช้งานระดับผู้ดูแลระบบ โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ใช้การตรวจสอบ Domain ที่ลงท้ายด้วย .th ซึ่งเป็นของประเทศไทย พบว่ามีข้อมูลกว่า ๒๒๑ ล้านรายการ สามารถแบ่งได้เป็น ๑) หน่วยงานราชการ (go.th) จำนวน ๙๒,๖๙๖,๙๙๓ รายการ ๒) บริษัท/องค์กร (co.th) จำนวน ๙๓,๓๓๙,๙๒๔ รายการ ๓) สถาบันการศึกษา (ac.th) จำนวน ๔๗,๓๖๙,๙๖๐ รายการ ๔) องค์กรไม่แสวงผลกำไร (or.th) จำนวน ๑๒,๙๓๙,๙๕๓ รายการ ๕) หน่วยงานกองทัพ (.mi.th) จำนวน ๒,๙๑๖,๙๕๙ รายการ ๖) อื่น ๆ จำนวน ๑๓,๐๑๖,๙๗๓ รายการ รวมทั้งหมด ๒๒๑,๙๕๗,๙๕๙ รายการ

ซึ่งข้อมูลดังกล่าวอาจส่งผลให้เกิดความเสียหายต่อระบบอย่างร้ายแรงและถูกขโมยข้อมูลสำคัญต่าง ๆ รวมถึงข้อมูลส่วนบุคคลของหน่วยงานและประชาชน ถ้าหากผู้ไม่หวังดีได้นำชุดข้อมูลเป็นบัญชีผู้ใช้งานระดับผู้ดูแลระบบไปใช้ในการโจมตี ทั้งนี้ ข้อมูลบัญชีผู้ใช้งาน (Credential) ถูกขโมยหรือรั่วไหลเกิดจากสาเหตุต่าง ๆ สรุปได้ ดังนี้

๓.๑ การโจมตีแบบฟิชชิง (Phishing) โดยผู้ไม่หวังดีส่งอีเมล/เว็บไซต์ปลอม หลอกให้ผู้ใช้กรอกรหัสผ่านเอง

๓.๒ มัลแวร์/Keylogger โดยโปรแกรมแอบแฝงที่ถูกติดตั้งในเครื่องของผู้ใช้ แล้วดักจับข้อมูลการพิมพ์ เช่น รหัสผ่าน

๓.๓ Credential ถูกเก็บไว้อย่างไม่ปลอดภัย ซึ่งอาจเก็บไว้เป็น Plaintext หรือแชร์กันใช้งานหลายคนในไฟล์เปิดเผย เช่น Excel, Notepad

๓.๔ การใช้รหัสผ่านซ้ำ โดยอาจมีผู้ใช้นำรหัสผ่านเดียวกันไปใช้หลายระบบ หากระบบใดระบบหนึ่งถูกแฮก รหัสผ่านจะหลุดหมด

๓.๕ การตั้งรหัสผ่านไม่รัดกุม ใช้รหัสผ่านเดาง่าย เช่น ๑๒๓๔๕๖, password หรือชื่อหน่วยงาน เป็นต้น

๓.๖ ระบบไม่ได้บังคับใช้ MFA (Multi-Factor Authentication) ซึ่งทำให้ผู้ไม่หวังดีสามารถเข้าสู่ระบบได้ทันที หากได้รหัสผ่าน

๓.๗ รหัสผ่านหรือ Token ถูก Hard-code ไว้ในซอร์สโค้ด โดยเฉพาะในโค้ดที่แชร์ใน GitHub หรือระบบควบคุมเวอร์ชันต่าง ๆ

๓.๘ การรั่วไหลจากบุคลากรภายใน (Insider Threat) ผู้มีสิทธิ์เข้าถึงระบบนำข้อมูลออกไปโดยเจตนา หรือโดยประมาท

๓.๙ ระบบไม่มีการตรวจสอบหรือแจ้งเตือนความผิดปกติ ทำให้ไม่สามารถรู้ได้ทันทีว่ามีการใช้งาน Credential อย่างผิดปกติ

กมช. จึงได้เสนอแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย เพื่อเป็นการป้องกันไม่ให้หน่วยงานต่าง ๆ ที่อาจมีข้อมูลบัญชีผู้ใช้งาน (Credential) ถูกขโมยหรือรั่วไหล และทำให้ Hacker สามารถเข้าถึงระบบงานต่าง ๆ ของหน่วยงาน ตลอดจนโจมตีหน่วยงานเพื่อขโมยข้อมูลหรือเข้ารหัสข้อมูลส่งผลกระทบต่อการดำเนินงานหรือระบบงานต่าง ๆ และอาจจะส่งผลกระทบต่อระบบบริการต่าง ๆ ที่ให้บริการแก่ประชาชนได้ สกมช. จึงขอนำเสนอแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย

ทั้งนี้ ที่ประชุมมีมติ เห็นชอบแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ตามที่ กมช. เสนอ และมอบหมายให้ สกมช. เสนอแนวทางดังกล่าว ให้คณะรัฐมนตรีพิจารณาประกาศให้ทุกหน่วยงานถือปฏิบัติ ต่อไป

๔. <u>ประโยชน์และผลกระทบ</u>

การดำเนินการตามกรอบแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัยจะช่วยยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ในภาครัฐอย่างเป็นระบบ ส่งผลให้ระบบดิจิทัลของรัฐมีความมั่นคงปลอดภัยมากยิ่งขึ้น เพิ่มความเชื่อมั่นให้แก่ประชาชน ภาคธุรกิจ และนักลงทุน อีกทั้งยังเป็นการสนับสนุนนโยบายดิจิทัลของประเทศ ทำให้ประเทศไทยมีมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่ทัดเทียมกับระดับสากล

ผลกระทบที่จะเกิดขึ้น มาตรการนี้จะเพิ่มภาระบางส่วนต่อหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แต่จะช่วยลดความเสี่ยงด้านไซเบอร์ในระยะยาว ยกระดับความน่าเชื่อถือของบริการภาครัฐ เสริมสร้างความเชื่อมั่นของประชาชนและภาคธุรกิจ รวมถึงส่งเสริมความเชื่อมั่นต่อการลงทุนและความสามารถในการแข่งขันของประเทศด้านเศรษฐกิจดิจิทัล

๕. ค่าใช้จ่ายและแหล่งที่มา หรือภาวะสูญเสียรายได้

- ไม่มี

๖. ความเห็นหรือความเห็นชอบ/อนุมัติของหน่วยงานที่เกี่ยวข้อง

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้มีการจัดประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๑/๒๕๖๙ เมื่อวันที่ ๒๕ พฤษภาคม ๒๕๖๙ โดยมีระเบียบวาระที่ ๔.๕ เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย และที่ประชุมมีมติเห็นชอบแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เช่นการใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอและมอบหมายให้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เสนอแนวทางดังกล่าว ให้คณะรัฐมนตรีพิจารณาประกาศให้ทุกหน่วยงานถือปฏิบัติ ต่อไป

๗. ข้อกฎหมายและมติคณะรัฐมนตรีที่เกี่ยวข้อง

๗.๑ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๐) "คณะกรรมการมีหน้าที่และอำนาจ เสนอแนะและให้ความเห็นต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติหรือ คณะรัฐมนตรี เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์"

๗.๒ พระราชกฤษฎีกาว่าด้วยการเสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘

มาตรา ๔ วรรคหนึ่ง บัญญัติว่า "การเสนอเรื่องต่อคณะรัฐมนตรีให้เสนอได้ เฉพาะเรื่อง ดังต่อไปนี้

(๑) เรื่องที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของคณะรัฐมนตรีหรือให้ต้องเสนอคณะรัฐมนตรี"

มาตรา ๖ วรรคหนึ่ง บัญญัติว่า "การเสนอเรื่องต่อคณะรัฐมนตรีตามมาตรา ๔ ให้เป็นอำนาจของรัฐมนตรีเจ้าสังกัดเป็นผู้ลงนามเสนอเรื่อง เว้นแต่กรณีดังต่อไปนี้

(๑) ในกรณีที่คณะกรรมการใดมีนายกรัฐมนตรี รองนายกรัฐมนตรี หรือรัฐมนตรีประจำสำนักนายกรัฐมนตรี รัฐมนตรีว่าการกระทรวงหรือทบวงเป็นประธานกรรมการของคณะกรรมการนั้นให้นายกรัฐมนตรี รองนายกรัฐมนตรี รัฐมนตรีประจำสำนักนายกรัฐมนตรี รัฐมนตรีว่าการกระทรวงหรือทบวงแล้วแต่กรณี ในฐานะประธานกรรมการ เป็นผู้ลงนามเสนอเรื่องต่อคณะรัฐมนตรีได้

๗.๓ คำสั่งสำนักนายกรัฐมนตรี ที่ ๙๖/๒๕๖๙ ลงวันที่ ๒๔ เมษายน ๒๕๖๙ ให้มอบหมายและมอบอำนาจให้ รัฐมนตรีประจำสำนักนายกรัฐมนตรี (นายภราดร ปริศนานันทกุล) ปฏิบัติหน้าที่ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ แทนนายกรัฐมนตรี (สิ่งที่ส่งมาด้วย ๓)

๔. ข้อเสนอของหน่วยงานของรัฐ/คณะกรรมการเจ้าของเรื่อง

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติพิจารณาแล้ว ขอเสนอคณะรัฐมนตรีเพื่อโปรดพิจารณาให้ความเห็นชอบ ดังต่อไปนี้

๔.๑ เห็นชอบแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย

๔.๒ อนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงาน ต่อไป

จึงเรียนมาเพื่อโปรดพิจารณานำเสนอคณะรัฐมนตรีต่อไป

ขอแสดงความนับถือ

(นายกรวัศ ปริศนานันทกุล)
รัฐมนตรีประจำสำนักนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำเนาถูกต้อง

(นางสาวสมจิตร รูปเหมาะ)
นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ
๑๑ ธ.ค. ๖๗

สิ่งที่ส่งมาด้วย

https://drive.ncsa.or.th/s/32FMCZ5F2xteKxj

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
โทร. ๐๒ ๑๔๐ ๖๘๘๕
ไปรษณีย์อิเล็กทรอนิกส์ ncsc@ncsa.go.th



ด่วนที่สุด

ที่ อว (ปทร) ๐๖๐๓/๑๖๔๑๗

กระทรวงการอุดมศึกษา
วิทยาศาสตร์ วิจัยและนวัตกรรม
ถนนพระรามที่ ๖ เขตราชเทวี กทม. ๑๐๔๐๐

๑๑ สิงหาคม ๒๕๖๙

เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๗๕๘๕ ลงวันที่ ๔ สิงหาคม ๒๕๖๙

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะรัฐมนตรีขอให้กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม พิจารณาเสนอความเห็นในส่วนที่เกี่ยวข้องเพื่อประกอบการพิจารณาของคณะรัฐมนตรี เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ความละเอียดแจ้งแล้ว นั้น

กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ได้พิจารณาแล้วเห็นชอบด้วยกับแนวทางที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอในการนำระบบการยืนยันตัวตนแบบหลายปัจจัย (Multi - Factor Authentication: MFA) มาใช้เพื่อป้องกันการรั่วไหลของข้อมูลระบุตัวตน (Credential) อย่างไรก็ดี มีข้อคิดเห็นเพิ่มเติมว่า แม้การยืนยันตัวตนผ่านแอปพลิเคชัน ThaiD จะสามารถป้องกันการรั่วไหลของข้อมูลระบุตัวตน (Credential) ได้ แต่ระบบดังกล่าวยังอาจไม่ครอบคลุมถึงการป้องกันการรั่วไหลของข้อมูลส่วนบุคคล (Personal Data) เนื่องจากมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลจะขึ้นอยู่กับระบบรักษาความปลอดภัยของแอปพลิเคชันหรือหน่วยงานผู้พัฒนาแอปพลิเคชันนั้น ๆ เป็นสำคัญ จึงเห็นควรเสนอแนะให้กำหนดแนวทางหรือมาตรการคุ้มครองข้อมูลส่วนบุคคลเพิ่มเติม อาทิ การเข้ารหัสข้อมูล (Data Encryption) หรือการปกปิดข้อมูลบางส่วน (Data Masking) เป็นต้น

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

ขอแสดงความนับถือ

(นายยศชนัน วงศ์สวัสดิ์)
รัฐมนตรีว่าการกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม

สำนักงานปลัดกระทรวง
สำนักผู้ประสานงานคณะรัฐมนตรีและรัฐสภา
โทร ๐ ๒๓๓๓ ๓๗๐๐ ต่อ ๕๐๓๓
ไปรษณีย์อิเล็กทรอนิกส์ cplo@mhesi.go.th

สำเนาถูกต้อง

(นางสาวสมจิตร รูปเหมาะ)
นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ
๑๑ ส.ค. ๖๙

ด่วนที่สุด

ที่ คค(ปคร) ๐๖๑๐/๒๖๑



กระทรวงคมนาคม
ถนนราชดำเนินนอก กทม. ๑๐๑๐๐

๑๑ สิงหาคม ๒๕๖๙

เรื่อง การเสนอความเห็นแนวทางป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุการณ์บัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication : MFA)

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/๑๗๔๔๒ ลงวันที่ ๖ สิงหาคม ๒๕๖๙

ตามที่สำนักเลขาธิการคณะรัฐมนตรีขอให้กระทรวงคมนาคม เสนอความเห็นในส่วนที่เกี่ยวข้องเพื่อประกอบการพิจารณาของคณะรัฐมนตรี เรื่อง แนวทางป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้เสนอขอความเห็นชอบจากคณะรัฐมนตรี ความละเอียดแจ้งแล้ว นั้น

กระทรวงคมนาคม พิจารณาแล้ว มีความเห็นว่า ไม่ขัดข้องกับแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย รวมทั้งการให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงานต่อไป เนื่องจากจะทำให้เกิดการยกระดับมาตรการป้องกันภัยคุกคามทางไซเบอร์ของหน่วยงานภาครัฐอย่างเป็นระบบ ลดความเสี่ยงการรั่วไหลของข้อมูลส่วนบุคคล และช่วยเพิ่มความเชื่อมั่นให้กับประชาชนในการใช้บริการของหน่วยงานภาครัฐ

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายพิพัฒน์ รัชกิจประการ)
รัฐมนตรีว่าการกระทรวงคมนาคม

สำนักงานปลัดกระทรวง
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทร. ๐ ๒๒๘๓ ๓๓๖๖
ไปรษณีย์อิเล็กทรอนิกส์ sakmaorng.m@mot.go.th

สำเนาถูกต้อง
(นางสาวสมจิตร รูปเหมาะ)
นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ
๑๑ ส.ค. ๖๙

ที่ สธ ๐๒๐๑/ว๔๕๗๙

กระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๗ สิงหาคม ๒๕๖๕

เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว๒๕) ๑๑๕๘๕ ลงวันที่ ๔ สิงหาคม ๒๕๖๕

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะรัฐมนตรี ขอให้กระทรวงสาธารณสุขให้ความเห็นในส่วนที่เกี่ยวข้อง เพื่อประกอบการพิจารณาของคณะรัฐมนตรี ประเด็นความเห็น เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ความละเอียดแจ้งแล้ว นั้น

กระทรวงสาธารณสุขพิจารณาแล้วเห็นว่า เพื่อให้หน่วยงานในสังกัดที่มีการเก็บรวบรวม ใช้ และประมวลผลข้อมูลสุขภาพส่วนบุคคล มีมาตรการป้องกันข้อมูลบัญชีผู้ใช้งาน (Credential) รั่วไหล อันจะช่วยลดความเสี่ยงทางไซเบอร์และป้องกันการละเมิดข้อมูลส่วนบุคคลในภาคสาธารณสุขได้ในระยะยาว ตลอดจนยกระดับความเชื่อมั่นและความปลอดภัยในการให้บริการประชาชน ซึ่งสอดคล้องกับนโยบายของกระทรวงสาธารณสุขที่ให้ความสำคัญกับความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล จึงเห็นชอบในหลักการของแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ตามที่สำนักงานคณะกรรมการการวิจัยทางความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ อย่างไรก็ตาม การนำมาตรการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) มาปรับใช้ เช่น การใช้แอปพลิเคชัน ThaiD เป็นช่องทางหลัก ควรจะควบคู่กับการจัดเตรียมช่องทางการยืนยันตัวตนทางเลือกสำรองที่สามารถรองรับการพิสูจน์และยืนยันตัวตนผ่าน Digital ID อื่น ๆ หรือวิธีการยืนยันตัวตนรูปแบบอื่นที่มีมาตรฐานความมั่นคงปลอดภัย เพื่อความยืดหยุ่นและสนับสนุนความต่อเนื่องในการปฏิบัติงาน นอกจากนี้ แนวทางการป้องกันดังกล่าวอาจจะเพิ่มภาระให้กับหน่วยงานของรัฐ ดังนั้น สำนักงานคณะกรรมการการวิจัยทางความมั่นคงปลอดภัยไซเบอร์แห่งชาติและหน่วยงานที่เกี่ยวข้อง จึงควรมีมาตรการส่งเสริม ช่วยเหลือ และสนับสนุน หน่วยงานของรัฐ ทั้งในระยะสั้น ระยะกลาง และระยะยาว อย่างเป็นรูปธรรม ต่อไปด้วย

จึงเรียนมาเพื่อโปรดพิจารณาและดำเนินการต่อไปด้วย จะเป็นพระคุณ

ขอแสดงความนับถือ

(นายอัฒนา พร้อมพัฒน์)
รัฐมนตรีว่าการกระทรวงสาธารณสุข

สำนักงานปลัดกระทรวงสาธารณสุข
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทร. ๐ ๒๕๙๐ ๑๒๓๓
โปรยณีย์อีเมล์ saraban0212@moph.go.th

สำเนาถูกต้อง

(นางสาวณจิตร รูปเหมาะ)
นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ
๑๑ ส.ค. ๖๕

ด่วนที่สุด
ที่ นร ๐๗๐๔/๕๖๖

สำนักงบประมาณ
๑๐๖๓ ถนนพหลโยธิน
แขวงพญาไท กรุงเทพฯ ๑๐๔๐๐

๑๐ สิงหาคม ๒๕๖๙

เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ส) ๑๗๕๘๕ ลงวันที่ ๔ สิงหาคม ๒๕๖๙

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะรัฐมนตรีขอให้สำนักงบประมาณเสนอความเห็นในส่วนที่เกี่ยวข้องเพื่อประกอบการพิจารณาของคณะรัฐมนตรี กรณีคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอเรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย เพื่อให้คณะรัฐมนตรีพิจารณา ดังนี้

๑. เห็นชอบแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย

๒. อนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงานต่อไป

ความละเอียดแจ้งแล้ว นั้น

สำนักงบประมาณพิจารณาแล้วขอเรียนว่า แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย มีวัตถุประสงค์เพื่อยกระดับมาตรการป้องกันข้อมูลส่วนบุคคล

./และถด...

และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในภาครัฐอย่างเป็นระบบ อันจะส่งผลให้ระบบดิจิทัลของรัฐมีความมั่นคงปลอดภัย รวมถึงส่งเสริมความเชื่อมั่นต่อการลงทุนและความสามารถในการแข่งขันของประเทศด้านเศรษฐกิจดิจิทัล ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้มีมติเห็นชอบแนวทางดังกล่าว ในคราวประชุมครั้งที่ ๑/๒๕๖๙ เมื่อวันที่ ๒๕ พฤษภาคม ๒๕๖๙ แล้ว จึงเห็นสมควรที่คณะรัฐมนตรีจะพิจารณาให้ความเห็นชอบแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเทคนิคบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย และอนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงาน ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ สำหรับค่าใช้จ่ายที่จะเกิดขึ้น เห็นควรให้หน่วยงานที่เกี่ยวข้องใช้จ่ายจากงบประมาณรายจ่ายประจำปีที่ได้รับจัดสรร หรือพิจารณาปรับแผนการปฏิบัติงานและแผนการใช้จ่ายงบประมาณ โดยโอนงบประมาณรายจ่ายโอนเงินจัดสรรหรือเปลี่ยนแปลงเงินจัดสรร ตามระเบียบว่าด้วยการบริหารงบประมาณ พ.ศ. ๒๕๖๒ และที่แก้ไขเพิ่มเติม แล้วแต่กรณี หรือจัดทำแผนการปฏิบัติงานและแผนการใช้จ่ายงบประมาณ เพื่อเสนอขอตั้งงบประมาณรายจ่ายประจำปีตามความจำเป็นและเหมาะสมตามขั้นตอนต่อไป ทั้งนี้ หน่วยงานควรทบทวนจำนวนผู้ใช้งานระบบต่าง ๆ ให้เป็นปัจจุบัน และกำหนดสิทธิ์การเข้าถึงระบบและข้อมูลเท่าที่จำเป็น รวมถึงพิจารณาบังคับใช้มาตรการยืนยันตัวตนหลายปัจจัย สำหรับผู้ดูแลระบบ (Administrator) และบัญชีที่มีสิทธิ์ในการเข้าถึงข้อมูลระดับสูงในลำดับแรกก่อน

จึงเรียนมาเพื่อโปรดนำเสนอความเห็นประกอบการพิจารณาของคณะรัฐมนตรีต่อไป

ขอแสดงความนับถือ

(นายอนันต์ แก้วกำเนิด)
ผู้อำนวยการสำนักงบประมาณ

กองจัดทำงบประมาณด้านเศรษฐกิจ ๓
โทร. ๐ ๒๒๗๔ ๗๐๐๐ ต่อ ๑๔๔๘
ไปรษณีย์อิเล็กทรอนิกส์ saraban@bb.go.th

สำเนาถูกต้อง
(นางสาวสมจิตร รูปเหมาะ)
นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ
๑๑ มิ.ย. ๖๙

ด่วนที่สุด

ที่ นร ๑๑๑๖/๓๔๑๓



สำนักงานสภาพัฒนาการ
เศรษฐกิจและสังคมแห่งชาติ
๔๖๒ ถนนกรุงเกษม กรุงเทพฯ ๑๐๑๐๐

๑๓ สิงหาคม ๒๕๖๙

เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๗๕๘๕ ลงวันที่ ๔ สิงหาคม ๒๕๖๙

ตามที่สำนักเลขาธิการคณะรัฐมนตรีขอให้สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ เสนอความเห็นในส่วนที่เกี่ยวข้องเพื่อประกอบการพิจารณาของคณะรัฐมนตรี เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ที่เสนอโดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ความละเอียดแจ้งแล้วนั้น

สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติพิจารณาแล้ว มีความเห็นดังนี้

๑. เห็นควรให้ความเห็นชอบแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ

๒. เห็นควรอนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงาน ต่อไป

๓. อย่างไรก็ตาม เนื่องจากความพร้อมด้านงบประมาณและบุคลากรที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานแตกต่างกัน การบังคับใช้พร้อมกันทุกหน่วยงานรัฐในทันทีอาจเป็นไปได้ยากในทางปฏิบัติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ควรกำหนดระยะเวลาดำเนินการ (Roadmap) โดยมุ่งเน้นเร่งรัดหน่วยงานรัฐที่มีระบบบริการประชาชนขนาดใหญ่ ระบบที่มีความเสี่ยงสูง ระบบที่ถือครองข้อมูลส่วนบุคคลระดับอ่อนไหว และระบบสารสนเทศที่มีความสำคัญยิ่งยวด (Critical Information Infrastructure: CII) ตลอดจนระบบให้บริการประชาชนขนาดใหญ่ที่ยังขาดการติดตั้งใช้งานระบบการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) ให้ดำเนินการเป็นลำดับแรกภายในกรอบเวลาเร่งด่วน เพื่อจำกัดความเสี่ยงและลดโอกาสการเกิดเหตุข้อมูลรั่วไหลในจุดสำคัญ ซึ่งอาจส่งผลกระทบต่อเนื่องเป็นวงกว้าง และสร้างความเสียหายอย่างร้ายแรงต่อระบบงานภาครัฐรวมถึงประชาชนในภาพรวม

/๔. เพื่อให้...

๔. เพื่อให้การขับเคลื่อนมาตรการดังกล่าวเป็นไปอย่างมีประสิทธิภาพและลดภาระงบประมาณในภาพรวมของรัฐ ควรส่งเสริมให้หน่วยงานภาครัฐพิจารณาใช้โครงสร้างพื้นฐานกลาง หรือซอฟต์แวร์รหัสเปิด (Open Source) เป็นทางเลือกแรก โดยเฉพาะหน่วยงานขนาดเล็กหรือองค์กรปกครองส่วนท้องถิ่นที่มีข้อจำกัดด้านงบประมาณและบุคลากร เว้นแต่ระบบงานที่มีลักษณะเฉพาะ ระบบที่มีความมั่นคงปลอดภัยสูงพิเศษ หรือระบบที่ไม่รองรับการเชื่อมต่อกับระบบกลาง ให้หน่วยงานสามารถจัดหาหรือใช้ระบบการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) อื่นที่เหมาะสมตามมาตรฐานสากลได้ โดย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ควรหารือร่วมกับสำนักงานพัฒนารัฐบาลดิจิทัล หรือ สพร. ในการสนับสนุนด้านเทคนิค ยกระดับเสถียรภาพระบบเชื่อมโยงข้อมูลกลาง (Application Programming Interface : API) จัดทำชุดระบบต้นแบบ และจัดทำคู่มือมาตรฐานการนำไปปฏิบัติเพื่อช่วยอำนวยความสะดวกแก่หน่วยงานรัฐที่มีข้อจำกัดด้านงบประมาณและบุคลากร ตลอดจนกำชับให้มีการจัดเตรียมมาตรการทางเลือกรองรับประชาชนผู้รับบริการที่ไม่สามารถเข้าถึงสมาร์ทโฟนหรือแอปพลิเคชันดิจิทัล เพื่อไม่ให้มาตรการรักษาความมั่นคงปลอดภัยกลายเป็นอุปสรรคในการเข้าถึงบริการภาครัฐ

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายดนุชา พิชยนันท์)
เลขาธิการสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทร. ๐ ๒๒๘๐ ๔๐๘๕ ต่อ ๕๔๐๓
E-mail : Archan@nesdc.go.th

สำเนาถูกต้อง
(นางสาวสมจิตร รูปเหมาะ)
นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ
๑๕ ต.ค. ๖๗

ด่วน

ที่ สพร ๒๕๖๙/๑๓๗๕

๓๐ สิงหาคม ๒๕๖๙

เรื่อง ขอเสนอความเห็นต่อแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล)๑๗๔๔๕ ลงวันที่ ๔ สิงหาคม ๒๕๖๙

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะรัฐมนตรี ได้ขอให้สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร. พิจารณาเสนอความเห็นในส่วนที่เกี่ยวข้องกับแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้Digital Identity (ThaiD) หรือ ส่วนอื่นที่เห็นสมควรเพื่อประกอบการพิจารณาของคณะรัฐมนตรี ความละเอียดแจ้งแล้ว นั้น

ในการนี้ สพร. พิจารณาแล้ว เห็นด้วยในหลักการกับแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย เนื่องจากการยืนยันตัวตนหลายปัจจัยช่วยลดความเสี่ยงจากการนำข้อมูลบัญชีผู้ใช้งานที่ถูกขโมยหรือรั่วไหลไปใช้เข้าถึงระบบงานและข้อมูลโดยมิชอบ และเป็นการยกระดับความมั่นคงปลอดภัยของบริการดิจิทัลภาครัฐ โดยมีความเห็นเพิ่มเติมเพื่อประกอบการพิจารณา ดังนี้

๑. แนวทางดังกล่าวสอดคล้องกับมาตรฐานรัฐบาลดิจิทัล มรด. ๑-๒ : ๒๕๖๔ (DGS 1-2 : 2564) ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่อง การใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัลสำหรับบุคคลธรรมดาที่มีสัญชาติไทย (เวอร์ชัน ๑.๐) ซึ่งกำหนดให้การยืนยันตัวตนแบบหลายปัจจัยเป็นการยืนยันตัวตนที่ระดับความน่าเชื่อถือ AAL2 ทั้งนี้ ในการนำแนวทางดังกล่าวไปใช้ หน่วยงานควรกำหนดระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนให้เหมาะสมกับระดับความเสี่ยง ลักษณะของบริการ และผลกระทบที่อาจเกิดขึ้นจากการเข้าถึงบริการหรือข้อมูลโดยมิชอบ

หน่วยงานสามารถพิจารณาใช้ "ทางรัฐ ID" เป็นทางเลือกสำหรับการพิสูจน์และยืนยันตัวตนในการให้บริการภาครัฐ โดยทางรัฐ ID มีกระบวนการพิสูจน์และยืนยันตัวตนที่สอดคล้องกับมาตรฐานรัฐบาลดิจิทัลฉบับดังกล่าว และรองรับการยืนยันตัวตนหลายปัจจัย ซึ่งจะช่วยลดภาระของหน่วยงานในการ

พัฒนาระบบ...

อาคาร ๑๒๐ ชั้นที่ ๓ ชั้นที่ ๘ - ๙ และ ๑๑ ศูนย์ราชการเฉลิมพระเกียรติฯ ๗๐ พรรษา ถนนแจ้งวัฒนะ ๗ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐
120 Moo 3, 8th-9th Floor, Government Complex Commemorating His Majesty The King's 80th Birthday Anniversary (Building C),
Chaeng Watthana 7, Chaeng Watthana Road, Thung Song Hong, Lak Si, Bangkok 10210
โทร (+๖๖) ๐ ๒๕๕๒ ๖๐๖๐ อีเมล์: saraban@dga.or.th ศูนย์บริการ (+๖๖) ๐ ๒๕๕๒ ๑๐๖๐ อีเมล์: contact@dga.or.th
www.dga.or.th

พัฒนาระบบพิสูจน์และยืนยันตัวตนขึ้นใหม่ รวมทั้งสนับสนุนการให้บริการดิจิทัลภาครัฐมีมาตรฐาน และสามารถเชื่อมโยงการทำงานร่วมกันได้

๒. การใช้ Digital ID และการยืนยันตัวตนหลายปัจจัยสามารถควบคุมและลดความเสี่ยงจากการรั่วไหลของบัญชีผู้ใช้งานได้ในระดับหนึ่ง อย่างไรก็ดี มาตรการดังกล่าวมุ่งควบคุมการเข้าถึงระบบโดยบุคคลเป็นหลัก ขณะที่ระบบสารสนเทศของหน่วยงานอาจมีช่องทางการเข้าถึงในรูปแบบอื่น โดยเฉพาะ API ที่เปิดให้ระบบของหน่วยงานอื่นสามารถเชื่อมโยงและแลกเปลี่ยนข้อมูล ซึ่งอาจไปได้ผ่านกระบวนการยืนยันตัวตนของบุคคลโดยตรง หน่วยงานจึงควรกำหนดมาตรการควบคุมการเข้าถึง API และช่องทางเชื่อมโยงระบบควบคู่กัน ตามแนวทางที่กำหนดไว้ในมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล (Thailand Government Information Exchange Standard, Series: Linkage Standard) (มสพร. ๑๐ : ๒๕๖๖) มาตรการดังกล่าวควรครอบคลุมอย่างน้อย การเข้ารหัสข้อมูลระหว่างรับส่งด้วย TLS การพิสูจน์ตัวตนและกำหนดสิทธิของระบบที่เชื่อมโยง การจำกัดสิทธิให้สามารถเข้าถึงเฉพาะข้อมูลและบริการที่จำเป็น การจัดเก็บและบริหารจัดการข้อมูลสำหรับยืนยันตัวตนของระบบ (Credential) อย่างมั่นคงปลอดภัย การบันทึกและตรวจสอบข้อมูลการใช้งาน (Log) ตลอดจนการเฝ้าระวังและตรวจจับการเรียกใช้งานที่ผิดปกติ ทั้งนี้ หน่วยงานอาจพิจารณาเชื่อมโยงระบบผ่านเครือข่าย DG Link ที่สพร. ให้บริการ ตามความเหมาะสม เพื่อเพิ่มความมั่นคงปลอดภัยของช่องทางการเชื่อมโยงระหว่างหน่วยงาน

จึงเรียนมาเพื่อโปรดพิจารณาประกอบการเสนอคณะรัฐมนตรีต่อไป

ขอแสดงความนับถือ

(นางสาวอภิณห์พร อัจฉกมลเศรษฐ์)
รองผู้อำนวยการ รักษาการแทน
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

สำนักผู้อำนวยการ
กลุ่มงานพิเศษเฉพาะเรื่องและติดตามนโยบาย
โทรศัพท์ ๐๔ ๐๐๔๕ ๓๔๖๒ (พิมพ์ลักษณ์)
ไปรษณีย์อิเล็กทรอนิกส์สารบรรณกลาง saraban@dga.or.th

สำเนาถูกต้อง
สมจิตร รูปเหมาะ
(นางสาวสมจิตร รูปเหมาะ)
นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ
๑๑ ธ.ค. ๖๘