ด่วนที่สุด

ที่ อต ๐๐๒๓.๓/ว ๗๖๑๗

ศาลากลางจังหวัดอุตรดิตถ์
ถนนประชานิมิตร อต ๕๓๐๐๐

๒ กันยายน ๒๕๖๙

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และมาตรการคุ้มครองข้อมูลส่วนบุคคล เพื่อป้องกันเฝ้าระวัง และรับมือภัยคุกคามทางไซเบอร์และเตรียมความพร้อมรับการค้นหาช่องโหว่ของระบบการลงทะเบียนและฐานข้อมูลกิจการสภาเด็กและเยาวชนขององค์กรปกครองส่วนท้องถิ่น หรือระบบ CYCL

เรียน นายอำเภอ ทุกอำเภอ และนายกเทศมนตรีเมืองอุตรดิตถ์

อ้างถึง ๑. หนังสือจังหวัดอุตรดิตถ์ ด่วนมาก ที่ อต ๐๐๒๓.๓/ว ๔๖๑ ลงวันที่ ๑๒ พฤษภาคม ๒๕๖๙

สิ่งที่ส่งมาด้วย สำเนาหนังสือกรมส่งเสริมการปกครองท้องถิ่น ด่วนที่สุด ที่ มท ๐๘๑๖.๕/ว ๕๐๒๙ ลงวันที่ ๑ กันยายน ๒๕๖๙ จำนวน ๑ ชุด

ตามที่จังหวัดอุตรดิตถ์ แจ้งว่า กรมส่งเสริมการปกครองท้องถิ่นร่วมกับองค์การยูนิเซฟ ประเทศไทย ได้จัดทำระบบการลงทะเบียนและฐานข้อมูลกิจการสภาเด็กและเยาวชนขององค์กรปกครองส่วนท้องถิ่น หรือระบบ CYCL เพื่อสนับสนุน และส่งเสริมการมีส่วนร่วมของเด็กและเยาวชนในท้องถิ่นโดยใช้กลไกกิจการสภาเด็กและเยาวชน และได้แจ้งให้เทศบาลและองค์การบริหารส่วนตำบลทุกแห่ง มอบหมายเจ้าหน้าที่เป็นผู้ดูแลระบบ CYCL ระดับหน่วยงาน (เทศบาลและองค์การบริหารส่วนตำบล) เพื่อทำหน้าที่ติดตาม ตรวจสอบ และประเมินผลการดำเนินงานให้เป็นปัจจุบัน นั้น

จังหวัดอุตรดิตถ์ ได้รับแจ้งจากกรมส่งเสริมการปกครองท้องถิ่น ว่ากระทรวงมหาดไทย ขอให้หน่วยงานพิจารณาดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมาตรการคุ้มครองข้อมูลส่วนบุคคล และมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ทั้งนี้ ในส่วนของมาตรการเร่งด่วน ขอให้หน่วยงานเปลี่ยนรหัสผ่านเป็นประจำ ตลอดจนระงับบัญชีที่ไม่มีความจำเป็น และทบทวนสิทธิ์การเข้าถึงระบบอย่างเคร่งครัด ในการนี้ เพื่อให้การดำเนินการดังกล่าวบรรลุวัตถุประสงค์ จึงขอแจ้งให้เทศบาล และองค์การบริหารส่วนตำบล ทุกแห่งดำเนินการ ดังนี้

๑. ปฏิบัติตามแนวทางการดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมาตรการคุ้มครองข้อมูลส่วนบุคคล ตามข้อ ๔ ข้อ ๑๑ ข้อ ๑๔ และข้อ ๑๕ โดยเคร่งครัด

/๒. กำชับให้...

๒. กำชับให้เจ้าหน้าที่ผู้ดูแลระบบ CYCL ระดับหน่วยงาน (เทศบาลและองค์การบริหารส่วนตำบล) คณะบริหารสภาเด็กและเยาวชนตำบล/เทศบาล และสมาชิกสภาเด็กและเยาวชนตำบล/เทศบาล ซึ่งเป็นผู้ใช้งานระบบการลงทะเบียนและฐานข้อมูลกิจการสภาเด็กและเยาวชนขององค์กรปกครองส่วนท้องถิ่น โดยขอให้ดำเนินการกำหนดรหัสผ่านใหม่ (เปลี่ยนรหัสผ่าน) ตามหลักเกณฑ์ที่กำหนด ทั้งนี้ ตั้งแต่วันที่ ๑ กันยายน ๒๕๖๙ เป็นต้นไป รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อพิจารณา สำหรับอำเภอ ขอให้แจ้งองค์กรปกครองท้องถิ่นในพื้นที่ทราบและดำเนินการต่อไป

ขอแสดงความนับถือ

(นายสรพงษ์ มานะสุขอนันต์)
รองผู้ว่าราชการจังหวัด ปฏิบัติราชการแทน
ผู้ว่าราชการจังหวัดอุตรดิตถ์

สำนักงานท้องถิ่นจังหวัด
กลุ่มงานส่งเสริมและพัฒนาท้องถิ่น
โทร. ๐-๕๕๔๐-๓๐๐๘ ต่อ ๓
ผู้ประสานงาน : ธนาภรณ์ เปรมปรี (โทร.) ๐๘๙-๔๓๙๐๙๒๗

"ร่วมเฉลิมฉลอง ๑๑๑ ปี จังหวัดอุตรดิตถ์"

ด่วนที่สุด

ที่ มท ๐๘๑๖.๕/ว ๔๐๒๙

กรมส่งเสริมการปกครองท้องถิ่น
ถนนนครราชสีมา เขตดุสิต กทม. ๑๐๓๐๐

๑ กันยายน ๒๕๖๙

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และมาตรการคุ้มครองข้อมูลส่วนบุคคล เพื่อป้องกัน เฝ้าระวัง และรับมือภัยคุกคามทางไซเบอร์และเตรียมความพร้อมรับการค้นหาช่องโหว่ของระบบการลงทะเบียนและฐานข้อมูลกิจการสภาเด็กและเยาวชนขององค์กรปกครองส่วนท้องถิ่น หรือระบบ CYCL

เรียน ผู้ว่าราชการจังหวัด ทุกจังหวัด

อ้างถึง ๑. หนังสือกรมส่งเสริมการปกครองท้องถิ่น ด่วนมาก ที่ มท ๐๘๑๖.๕/ว ๔๖๓๐ ลงวันที่ ๗ สิงหาคม ๒๕๖๙
๒. หนังสือกรมส่งเสริมการปกครองท้องถิ่น ด่วนมาก ที่ มท ๐๘๑๖.๕/ว ๒๑๗๘ ลงวันที่ ๘ พฤษภาคม ๒๕๖๙
๓. หนังสือกรมส่งเสริมการปกครองท้องถิ่น ที่ มท ๐๘๑๖.๕/ว ๒๔๗๖ ลงวันที่ ๑๐ มิถุนายน ๒๕๖๗

สิ่งที่ส่งมาด้วย ๑. สำเนาหนังสือกระทรวงมหาดไทย ด่วนที่สุด ที่ มท ๐๒๑๐.๕/ว ๗๐๗๙
ลงวันที่ ๑๙ สิงหาคม ๒๕๖๙ จำนวน ๑ ฉบับ
๒. แนวทางการตั้งและเปลี่ยนรหัสผ่านระบบ CYCL จำนวน ๑ ชุด
๓. ขั้นตอนการเปลี่ยนรหัสผ่านระบบ CYCL จำนวน ๑ ชุด

ตามหนังสือที่อ้างถึง กรมส่งเสริมการปกครองท้องถิ่นร่วมกับองค์การยูนิเซฟ ประเทศไทย ได้จัดทำระบบการลงทะเบียนและฐานข้อมูลกิจการสภาเด็กและเยาวชนขององค์กรปกครองส่วนท้องถิ่น หรือระบบ CYCL เพื่อสนับสนุนและส่งเสริมการมีส่วนร่วมของเด็กและเยาวชนในท้องถิ่นโดยใช้กลไกกิจการสภาเด็กและเยาวชน และขอความร่วมมือจังหวัด มอบหมายเจ้าหน้าที่เป็นผู้ดูแลระบบ CYCL ระดับจังหวัด พร้อมทั้งแจ้งเทศบาลและองค์การบริหารส่วนตำบลทุกแห่ง มอบหมายเจ้าหน้าที่เป็นผู้ดูแลระบบ CYCL ระดับหน่วยงาน (เทศบาลและองค์การบริหารส่วนตำบล) เพื่อทำหน้าที่ติดตาม ตรวจสอบ และประเมินผลการดำเนินงานให้เป็นปัจจุบัน ประกอบกับได้จัดประชุมชี้แจงการใช้งานระบบการลงทะเบียนและฐานข้อมูลกิจการสภาเด็กและเยาวชนขององค์กรปกครองส่วนท้องถิ่น ปี พ.ศ. ๒๕๖๙ ให้กับเจ้าหน้าที่ผู้ดูแลระบบ CYCL ระดับจังหวัดแล้ว นั้น

กรมส่งเสริมการปกครองท้องถิ่นได้รับแจ้งจากกระทรวงมหาดไทย ขอให้หน่วยงานพิจารณาดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมาตรการคุ้มครองข้อมูลส่วนบุคคล และมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ทั้งนี้ ในส่วนของมาตรการเร่งด่วน ขอให้หน่วยงานเปลี่ยนรหัสผ่านเป็นประจำ ตลอดจนระงับบัญชีที่ไม่มีความจำเป็น และทบทวนสิทธิ์การเข้าถึงระบบอย่างเคร่งครัด ในการนี้ เพื่อให้การดำเนินการดังกล่าวบรรลุวัตถุประสงค์ จึงขอความร่วมมือจังหวัดแจ้งสำนักงานท้องถิ่นจังหวัด เทศบาล และองค์การบริหารส่วนตำบลทุกแห่ง ดำเนินการ ดังนี้

๑. ปฏิบัติตามแนวทางการดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมาตรการคุ้มครองข้อมูลส่วนบุคคล ตามข้อ ๔ ข้อ ๑๑ ข้อ ๑๔ และข้อ ๑๕ โดยเคร่งครัด

/๒. กำชับ ...

๒. กำชับให้เจ้าหน้าที่ผู้ดูแลระบบ CYCL ระดับจังหวัด (สำนักงานท้องถิ่นจังหวัด) และเจ้าหน้าที่ผู้ดูแลระบบ CYCL ระดับหน่วยงาน (เทศบาลและองค์การบริหารส่วนตำบล) คณะบริหารสภาเด็กและเยาวชนตำบล/เทศบาล และสมาชิกสภาเด็กและเยาวชนตำบล/เทศบาล ซึ่งเป็นผู้ใช้งานระบบการลงทะเบียนและฐานข้อมูลกิจการสภาเด็กและเยาวชนขององค์กรปกครองส่วนท้องถิ่น โดยขอให้ดำเนินการกำหนดรหัสผ่านใหม่ (เปลี่ยนรหัสผ่าน) ตามหลักเกณฑ์ที่กำหนด ทั้งนี้ ตั้งแต่วันที่ ๑ กันยายน ๒๕๖๙ เป็นต้นไป รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย โดยสามารถดาวน์โหลดได้ที่ QR Code ท้ายหนังสือนี้

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นายศิริพันธ์ ศรีกงพลี)
รองอธิบดี ปฏิบัติราชการแทน
อธิบดีกรมส่งเสริมการปกครองท้องถิ่น

กองการศึกษาท้องถิ่น
กลุ่มงานส่งเสริมการเรียนรู้และวัฒนธรรมท้องถิ่น
โทร. ๐ ๒๒๔๑ ๙๐๐๐ ต่อ ๕๓๓๗
ไปรษณีย์อิเล็กทรอนิกส์ saraban@dla.go.th
ผู้ประสานงาน ว่าที่ร้อยตรีไอยศูรย์ บุญมงคลโชค โทร. ๐๘ ๙๙๒๕ ๒๘๗๖
นางสาวเบญญาภา ปทุมสูติ โทร. ๐๙ ๓๓๔๑ ๔๗๓๐

ศูนย์เทคโนโลยีสารสนเทศ...
เลขรับ ๓๕๖๖
๑๙ ส.ค. 2569

กรมส่งเสริมการปกครองท้องถิ่น
เลขรับ 39337
วันที่ 19 ส.ค. 2569
เวลา.....

ด่วนที่สุด **บันทึกข้อความ**

ส่วนราชการ กระทรวงมหาดไทย สำนักงานปลัดกระทรวง ศูนย์เทคโนฯ โทร. ๐๒ ๒๘๑ ๑๕๖๗ ต่อ ๕๑๕๕๐

ที่ มท ๐๒๑๐.๕/ว ๒๑๐๔๗ **วันที่** ๑๙ สิงหาคม ๒๕๖๙

เรื่อง ขอให้พิจารณาดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมาตรการคุ้มครองข้อมูลส่วนบุคคล

เรียน หัวหน้าส่วนราชการระดับกรมและหัวหน้าหน่วยงานรัฐวิสาหกิจในสังกัดกระทรวงมหาดไทย

ด้วยเหตุการณ์ภัยคุกคามทางไซเบอร์และข้อมูลรั่วไหลที่เกิดขึ้นกับหน่วยงานภาครัฐ โดยวิธีการที่ผู้โจมตีได้นำข้อมูลบัญชีผู้ใช้งาน (Credential) สำหรับการยืนยันตัวตน ไปใช้เข้าถึงช่องทางเครือข่ายของระบบภายในหน่วยงานภาครัฐ ทำให้ผู้โจมตีสามารถเข้าถึงข้อมูลต่าง ๆ ของหน่วยงาน รวมถึงข้อมูลส่วนบุคคล ส่งผลกระทบให้เกิดความเสียหายต่อหน่วยงานภาครัฐและประชาชน กระทรวงดิจิทัลและเพื่อเศรษฐกิจและสังคม จึงกำหนดมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมาตรการคุ้มครองข้อมูลส่วนบุคคล เพื่อเป็นการยกระดับการป้องกันไม่ให้หน่วยงานภาครัฐถูกโจมตีระบบ ข้อมูลบัญชีผู้ใช้งาน (Credential) ถูกขโมย และป้องกันข้อมูลส่วนบุคคลรั่วไหล ประกอบกับในคราวการประชุมคณะรัฐมนตรี เมื่อวันที่ ๑๑ สิงหาคม ๒๕๖๙ ที่ประชุมมีมติเห็นชอบแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย

ในการนี้ กระทรวงมหาดไทยจึงขอให้หน่วยงานพิจารณาดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมาตรการคุ้มครองข้อมูลส่วนบุคคล และมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication : MFA) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ทั้งนี้ ในส่วนของมาตรการเร่งด่วนขอให้หน่วยงานเปลี่ยนรหัสผ่านเป็นประจำ ตลอดจนระงับบัญชีที่ไม่มีความจำเป็นและทบทวนสิทธิ์การเข้าถึงระบบอย่างเคร่งครัด โดยดำเนินการให้แล้วเสร็จภายในวันที่ ๒๑ สิงหาคม ๒๕๖๙ รายละเอียดตาม QR Code ท้ายหนังสือฉบับนี้

จึงเรียนมาเพื่อพิจารณาดำเนินการในส่วนที่เกี่ยวข้อง

กลุ่มงานระบบงานคอมพิวเตอร์
เลขรับ ๑๑๐๕
วันที่ ๒๑ ส.ค. ๒๕๖๙
เวลา.....น.

(นายนิรัตน์ พงษ์สิทธิถาวร)
รองปลัดกระทรวงมหาดไทย ปฏิบัติราชการแทน
ปลัดกระทรวงมหาดไทย

รายละเอียด

ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand

NCSA สกมช

ครม. เดินหน้า ยกระดับ MFA ทุกหน่วยงานรัฐ

เพิ่มเกราะป้องกันการสวมบัญชี
เมื่อ Username และ Password รั่วไหล

Multi-Factor Authentication: MFA
คือการยืนยันตัวตนมากกว่า 1 ขั้น
แม้รหัสผ่านรั่ว ผู้ไม่หวังดีก็เข้าใช้บัญชีได้ยากขึ้น

แผนขับเคลื่อน 30–60–90 วัน

ภายใน 30 วัน – สำรวจและจัดทำ Baseline

- **ยืนยันรายการระบบหรือ URL**
- สำรวจระบบสำคัญและข้อมูลส่วนบุคคล
- รายงานสถานะ MFA และแผนปรับปรุง

ภายใน 60 วัน – เร่งปรับปรุงระบบสำคัญ

- **เปิด MFA สำหรับ Admin / Privileged / Remote**
- เร่งระบบบริการประชาชนและ Internet-facing
- กำหนดมาตรการทดแทนสำหรับระบบเดิม

ภายใน 90 วัน – ขยายผลและวางมาตรฐานถาวร

- **ปิดช่องว่าง MFA ของระบบอื่นตามความเสี่ยง**
- ใช้ Website Security Standard
- ใช้ Cloud Security Standard กับระบบ Cloud

สิ่งที่ทุกหน่วยงานจะได้รับ

ลดความเสี่ยง
Force Reset Password และปิดระบบ/ลบข้อมูล หากไม่ใช้

เพิ่มความมั่นใจ
ระบบปลอดภัย เชื่อถือได้

พร้อมปฏิบัติตามนโยบาย
สอดคล้องกับมาตรฐานและข้อกำหนดภาครัฐ

“ MFA ไม่ใช่การะเพิ่ม แต่คือเกราะที่ทำให้องค์กรไทย มั่นคง ปลอดภัย และเชื่อถือได้ ”

มาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์
และมาตรการคุ้มครองข้อมูลส่วนบุคคล

ปัจจุบันภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับ การรั่วไหลของข้อมูลส่วนบุคคล (Data Leak) มีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง โดยพบว่ามีข้อมูลบัญชีผู้ใช้งานของหน่วยงาน เช่น ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ถูกเผยแพร่ในแหล่งต่าง ๆ เป็นจำนวนมาก ซึ่งข้อมูลที่รั่วไหลดังกล่าวสามารถถูกนำไปใช้ในการเข้าถึงระบบสารสนเทศ เว็บไซต์ สื่อสังคมออนไลน์ หรือแพลตฟอร์มที่เกี่ยวข้องโดยไม่ได้รับอนุญาต และอาจถูกใช้เป็นจุดเริ่มต้นในการเข้าถึงข้อมูลสำคัญ การยกระดับสิทธิ์ (Privilege Escalation) หรือการเคลื่อนย้ายภายในระบบเครือข่าย (Lateral Movement) ของหน่วยงาน

จากการเฝ้าระวังและติดตามสถานการณ์ พบว่าการเกิด Data Leak อาจมีสาเหตุมาจากหลายปัจจัย เช่น การโจมตีผ่านห่วงโซ่อุปทาน (Supply Chain Attack) การตั้งค่าระบบหรือเว็บไซต์ที่ไม่ปลอดภัย การขาดมาตรการป้องกันสำหรับระบบที่เปิดให้บริการจากภายนอก การติดมัลแวร์ประเภทขโมยข้อมูล (Infostealer) รวมถึงการรั่วไหลของข้อมูลผ่านระบบเชื่อมต่อ โปรแกรมประยุกต์ หรือผู้ให้บริการภายนอก เช่น การบริหารจัดการ Application Programming Interface (API) หรือการจัดเก็บข้อมูลรับรอง (Credentials) สำหรับการเชื่อมต่อที่ไม่เหมาะสม ซึ่งล้วนเป็นปัจจัยสำคัญที่นำไปสู่การรั่วไหลของข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์กร

นอกจากนี้ ยังพบว่าหลายหน่วยงานมีช่องโหว่ด้านการบริหารจัดการข้อมูลและสิทธิ์การเข้าถึง เช่น การกำหนดสิทธิ์ไม่เหมาะสม การมีบัญชีผู้ใช้งานที่ไม่ได้ใช้งานแต่ยังคงเปิดใช้งานอยู่ การไม่เพิกถอนสิทธิ์เมื่อมีการเปลี่ยนแปลงหน้าที่หรือพ้นสภาพการปฏิบัติงาน รวมถึงการขาดระบบบริหารจัดการบัญชีผู้ใช้งานแบบรวมศูนย์ (Identity and Access Management: IAM) ซึ่งเป็นปัจจัยเสริมที่ทำให้ข้อมูลส่วนบุคคลที่รั่วไหลสามารถถูกนำไปใช้ได้อย่างมีประสิทธิภาพโดยผู้ไม่ประสงค์ดี และเพิ่มความเสี่ยงต่อการละเมิดข้อมูล (Data Breach) ในวงกว้าง

<u>ประเด็นความเสี่ยงสำคัญที่หน่วยงานควรให้ความสำคัญ มีดังนี้</u>

๑. ความเสี่ยงด้านการควบคุมบุคลากรและสิทธิ์การเข้าถึง

ทั้งนี้ ในหลายหน่วยงานยังพบปัญหาด้านการบริหารจัดการสิทธิ์การเข้าถึงและบัญชีผู้ใช้งาน ซึ่งอาจก่อให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศ โดยมีประเด็นสำคัญ ดังนี้

- การกำหนดสิทธิ์การเข้าถึงไม่เหมาะสม หรือให้สิทธิ์เกินความจำเป็นต่อหน้าที่
- การมีบัญชีผู้ใช้งานที่ไม่ได้ใช้งานแต่ยังคงเปิดใช้งานอยู่ (บัญชีค้าง)
- การไม่ปรับสิทธิ์ให้สอดคล้องกับการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ
- การไม่เพิกถอนสิทธิ์โดยทันทีเมื่อบุคลากรพ้นสภาพการปฏิบัติงาน หรือหมดความจำเป็นในการเข้าถึงระบบ
- ความเสี่ยงจากการใช้งานบัญชีโดยไม่เหมาะสมจากบุคลากรภายใน ผู้รับจ้าง ที่ปรึกษา หรือผู้ให้บริการภายนอก
- การขาดการควบคุมและติดตามการใช้งานบัญชีผู้ดูแลระบบหรือบัญชีสิทธิ์ระดับสูงอย่างเพียงพอ

ทั้งนี้ ปัจจัยดังกล่าวอาจส่งผลให้ผู้ไม่ประสงค์ดีสามารถนำบัญชีผู้ใช้งานไปใช้ในการเข้าถึงข้อมูลหรือระบบสำคัญของหน่วยงานโดยไม่ได้รับอนุญาต หรือใช้งานเกินขอบเขตหน้าที่ที่กำหนด

ดังนั้น หน่วยงานควรกำหนดมาตรการควบคุมบัญชีผู้ใช้งานและสิทธิ์การเข้าถึงอย่างเป็นระบบ โดยครอบคลุมประเด็นสำคัญ ดังนี้

- การกำหนดและอนุมัติสิทธิ์เมื่อเริ่มปฏิบัติงาน
- การปรับเปลี่ยนสิทธิ์เมื่อมีการโยกย้ายหรือเปลี่ยนแปลงหน้าที่
- การแยกหน้าที่ความรับผิดชอบที่สำคัญออกจากกัน (Segregation of Duties)
- การควบคุมและติดตามการใช้งานบัญชีสิทธิ์ระดับสูง
- การระงับหรือเพิกถอนสิทธิ์โดยทันทีเมื่อพ้นสภาพการปฏิบัติงาน
- กำหนดนโยบายรหัสผ่านที่ปลอดภัย เช่น หลีกเลี่ยงการใช้รหัสผ่านซ้ำ กำหนดรายการรหัสผ่านต้องห้าม (Blacklist) และส่งเสริมการใช้เครื่องมือจัดการรหัสผ่าน (Password Manager)
- กำหนดกระบวนการเปลี่ยนและกู้คืนรหัสผ่านอย่างปลอดภัย เช่น การยืนยันตัวตนก่อนรีเซ็ตรหัสผ่าน และจำกัดการใช้งานรหัสผ่านเดิม

๒. ความเสี่ยงจากการรั่วไหลของข้อมูลและการควบคุมการส่งออกข้อมูลไม่เพียงพอ

นอกจากนี้ สภาพแวดล้อมการใช้งานระบบสารสนเทศในปัจจุบันมีความซับซ้อนและเชื่อมโยงกันหลายระบบ ทำให้มีการรับส่ง จัดเก็บ และใช้งานข้อมูลผ่านหลายช่องทาง ทั้งระบบภายใน ระบบคลาวด์ อีเมล เว็บแอปพลิเคชัน ระบบแชร์ไฟล์ อุปกรณ์พกพา และโปรแกรมเว็บเบราว์เซอร์ หากหน่วยงานขาดมาตรการกำกับดูแลข้อมูลอย่างเหมาะสม อาจส่งผลให้ข้อมูลสำคัญถูกเปิดเผย เข้าถึง ใช้งาน หรือส่งออกไปยังภายนอกโดยไม่ได้รับอนุญาต

โดยความเสี่ยงที่พบบ่อย มีดังนี้

- การกำหนดสิทธิ์เข้าถึงข้อมูลไม่เหมาะสม หรือเปิดให้เข้าถึงกว้างเกินความจำเป็น
- การจัดเก็บข้อมูลสำคัญในระบบหรือพื้นที่ที่ไม่ปลอดภัย
- การรับส่งข้อมูลโดยไม่มีการเข้ารหัส หรือใช้ช่องทางที่ไม่ปลอดภัย
- การใช้งานระบบคลาวด์ อีเมล หรือระบบแชร์ไฟล์ โดยไม่มีมาตรการควบคุมที่เพียงพอ
- การขาดมาตรการควบคุมและเฝ้าระวังการนำข้อมูลออกจากระบบ
- การใช้รหัสผ่านซ้ำ หรือจัดเก็บข้อมูลบัญชีและกุญแจสำหรับเชื่อมต่อระบบในลักษณะที่ไม่เหมาะสม
- ความเสี่ยงจากโปรแกรมเว็บเบราว์เซอร์ เช่น การบันทึกรหัสผ่าน การถูกขโมย session token หรือ cookie และการใช้งานส่วนขยายที่ไม่ปลอดภัย
- การติดมัลแวร์ประเภทขโมยข้อมูลที่สามารถดึงข้อมูลบัญชีผู้ใช้งานหรือข้อมูลสำคัญจากเครื่องผู้ใช้งาน

ดังนั้น หน่วยงานควรกำหนดมาตรการป้องกันการรั่วไหลของข้อมูลอย่างเป็นระบบ โดยครอบคลุมประเด็นสำคัญ ดังนี้

- จำแนกประเภทข้อมูลตามระดับความสำคัญ (Data Classification) และกำหนดแนวทางการใช้งานข้อมูลอย่างเหมาะสม
- จำกัดสิทธิ์การเข้าถึงข้อมูลตามหน้าที่และความจำเป็น (Least Privilege)
- เข้ารหัสข้อมูลทั้งขณะจัดเก็บและขณะรับส่ง (Encryption at Rest และ In Transit)
- ควบคุมการใช้งานอีเมล ระบบคลาวด์ ระบบแชร์ไฟล์ และช่องทางรับส่งข้อมูลอื่นอย่างรัดกุม
- หลีกเลี่ยงการจัดเก็บรหัสผ่านหรือข้อมูลรับรองไว้ในเว็บเบราว์เซอร์หรือพื้นที่ที่เข้าถึงได้ง่าย
- ควบคุมการติดตั้งและใช้งานส่วนขยายของเว็บเบราว์เซอร์เท่าที่จำเป็น
- เฝ้าระวัง ตรวจสอบ และควบคุมการนำข้อมูลออกจากระบบ (Data Loss Prevention)
- ตรวจสอบและป้องกันมัลแวร์ที่มุ่งขโมยข้อมูลจากอุปกรณ์ผู้ใช้งานอย่างสม่ำเสมอ

๓. ความเสี่ยงจากการตั้งค่าระบบเว็บไซต์และระบบที่เปิดให้บริการจากภายนอกไม่เหมาะสม

ทั้งนี้ ระบบเว็บไซต์ เว็บเซิร์ฟเวอร์ และระบบสารสนเทศที่เปิดให้บริการจากภายนอก มักเป็นเป้าหมายหลักของการโจมตีจากผู้ไม่ประสงค์ดี หากมีการตั้งค่าที่ไม่เหมาะสม หรือขาดการดูแลรักษาความมั่นคงปลอดภัยอย่างต่อเนื่อง อาจส่งผลให้เกิดความเสี่ยงต่อการถูกโจมตีและเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยมีประเด็นสำคัญ ดังนี้

- การตั้งค่าระบบไม่เหมาะสม หรือเปิดใช้งานบริการและพอร์ตที่ไม่จำเป็น
- การไม่ปรับปรุงซอฟต์แวร์ ระบบจัดการเนื้อหา (CMS) เฟรมเวิร์ก หรือปลั๊กอินให้เป็นปัจจุบัน
- การขาดมาตรการเสริมความมั่นคงปลอดภัยสำหรับระบบที่เปิดให้บริการจากภายนอก
- การกำหนดสิทธิ์ของบัญชีบริการหรือบัญชีผู้ดูแลระบบไม่เหมาะสม
- ความเสี่ยงจากการถูกโจมตีผ่านช่องทางเว็บ เช่น การสแกนช่องโหว่ การเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือการแก้ไขหน้าเว็บไซต์
- การถูกใช้ระบบเป็นช่องทางแพร่กระจายมัลแวร์ หรือขโมยข้อมูลของหน่วยงานและผู้ใช้งาน

ทั้งนี้ ความเสี่ยงดังกล่าวอาจส่งผลให้ระบบของหน่วยงานถูกบุกรุก ถูกแก้ไขข้อมูล หรือถูกใช้เป็นจุดเริ่มต้นในการโจมตีระบบภายในของหน่วยงาน ดังนั้น หน่วยงานควรดำเนินการเสริมความมั่นคงปลอดภัยของระบบเว็บไซต์และระบบที่เปิดให้บริการจากภายนอกอย่างสม่ำเสมอ โดยครอบคลุมประเด็นสำคัญ ดังนี้

- ปิดบริการหรือพอร์ตที่ไม่จำเป็น และจำกัดการเข้าถึงเฉพาะที่จำเป็น
- ปรับแต่งค่าความมั่นคงปลอดภัยของระบบให้เหมาะสม (Secure Configuration)
- อัปเดตซอฟต์แวร์ ระบบจัดการเนื้อหา เฟรมเวิร์ก และส่วนประกอบที่เกี่ยวข้องให้เป็นปัจจุบันอยู่เสมอ
- จำกัดสิทธิ์ของบัญชีบริการและบัญชีผู้ดูแลระบบตามหลักความจำเป็น
- แยกส่วนระบบที่ให้บริการภายนอกออกจากระบบภายใน (Network Segmentation)
- พิจารณาใช้มาตรการป้องกันการโจมตีผ่านช่องทางเว็บ เช่น Web Application Firewall (WAF) หรือมาตรการที่เทียบเท่า

๔. ความเสี่ยงจากการรั่วไหลผ่านระบบเชื่อมต่อและ API

จากการเฝ้าระวังและติดตามสถานการณ์ภัยคุกคามทางไซเบอร์ พบว่าการรั่วไหลของบัญชีผู้ใช้งานอาจเกิดจากความเสี่ยงของระบบเชื่อมต่อและการใช้งาน Application Programming Interface (API) ซึ่งใช้ในการแลกเปลี่ยนข้อมูลระหว่างระบบทั้งภายในและภายนอกหน่วยงาน โดยมีประเด็นสำคัญ ดังนี้

- การกำหนดสิทธิ์การเข้าถึง API ไม่เหมาะสม หรือให้สิทธิ์เกินความจำเป็น
- การจัดเก็บข้อมูลรับรองสำหรับการเชื่อมต่อ เช่น API key, access token, secret key หรือบัญชีบริการ ในลักษณะที่ไม่ปลอดภัย
- การเปิดเผยข้อมูลรับรองในซอร์สโค้ด ไฟล์ตั้งค่า หรือระบบที่สามารถเข้าถึงได้โดยไม่จำเป็น
- การขาดการควบคุมและจำกัดการเข้าถึงระบบเชื่อมต่อกับผู้ให้บริการภายนอกหรือระบบคู่สัญญา
- การขาดการเฝ้าระวังการใช้งาน API ทำให้ไม่สามารถตรวจจับพฤติกรรมผิดปกติได้
- ความเสี่ยงจากการนำข้อมูลรับรองไปใช้เชื่อมต่อระบบ เข้าถึงข้อมูล หรือสั่งการผ่าน API โดยไม่ได้รับอนุญาต

ทั้งนี้ ความเสี่ยงดังกล่าวอาจส่งผลให้เกิดการเข้าถึงข้อมูลสำคัญ การใช้สิทธิ์เกินขอบเขต หรือการโจมตีระบบผ่านช่องทางการเชื่อมต่อระหว่างระบบ

ดังนั้น หน่วยงานควรกำหนดมาตรการควบคุมความมั่นคงปลอดภัยของระบบเชื่อมต่อและ API อย่างเหมาะสม โดยครอบคลุมประเด็นสำคัญ ดังนี้

- กำหนดสิทธิ์การเข้าถึง API ตามหลักความจำเป็น (Least Privilege)
- จัดเก็บ API key, token และข้อมูลรับรองในรูปแบบที่ปลอดภัย และหลีกเลี่ยงการฝังไว้ในซอร์สโค้ด
- ใช้กลไกการยืนยันตัวตนและการอนุญาตที่เหมาะสมสำหรับการเชื่อมต่อระหว่างระบบ
- จำกัดการเข้าถึง API ตามแหล่งที่มา เช่น IP address หรือ network ที่เชื่อถือได้
- เฝ้าระวังและตรวจสอบการใช้งาน API อย่างต่อเนื่อง เพื่อป้องกันและตรวจจับพฤติกรรมที่ผิดปกติ
- ทบทวนและยกเลิกข้อมูลรับรองหรือสิทธิ์การเข้าถึงที่ไม่จำเป็นอย่างสม่ำเสมอ

<u>แนวทางการดำเนินการตามมาตรการ</u>

จากการวิเคราะห์ประเด็นความเสี่ยงด้านการควบคุมบุคลากรและสิทธิ์การเข้าถึง การรั่วไหลของข้อมูล การตั้งค่าระบบเว็บไซต์และระบบที่เปิดให้บริการจากภายนอก รวมถึงความเสี่ยงจากระบบเชื่อมต่อและการแลกเปลี่ยนข้อมูลระหว่างระบบ หน่วยงานควรดำเนินมาตรการป้องกันและลดความเสี่ยงอย่างเป็นระบบ ครอบคลุมทั้งด้านเทคโนโลยี กระบวนการ และบุคลากร เพื่อป้องกันการนำข้อมูลบัญชีผู้ใช้งานไปใช้โดยมิชอบ และลดผลกระทบที่อาจเกิดขึ้นต่อระบบสารสนเทศของหน่วยงาน สามารถดำเนินการได้ ดังนี้

๑. ดำเนินการตรวจสอบและปิดช่องโหว่ของระบบสารสนเทศอย่างเร่งด่วน โดยเฉพาะระบบเว็บไซต์และบริการที่เปิดให้เข้าถึงจากภายนอก รวมถึงปรับแต่งค่าความมั่นคงปลอดภัยของระบบให้เหมาะสม ปิดบริการหรือพอร์ตที่ไม่จำเป็น และกำหนดมาตรการป้องกันการโจมตีผ่านช่องทางเว็บอย่างเหมาะสม

๒. สำรองข้อมูลอย่างน้อย ๓ ชุด และจัดเก็บข้อมูลสำรองในลักษณะที่แยกออกจากระบบหลัก รวมถึงมีการสำรองแบบออฟไลน์ เพื่อรองรับกรณีระบบถูกโจมตีหรือเกิดเหตุขัดข้องที่กระทบต่อความต่อเนื่องในการให้บริการ

๓. ตรวจสอบการเข้าถึงระบบจากระยะไกล เช่น Remote Desktop Protocol (RDP) และ Virtual Private Network (VPN) พร้อมเฝ้าระวังพฤติกรรมการใช้งานที่ผิดปกติ และกำหนดมาตรการยืนยันตัวตนที่เหมาะสมสำหรับการเข้าถึงจากภายนอก

๔. บังคับใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับระบบสำคัญ ระบบที่เปิดให้บริการจากภายนอก และบัญชีผู้ใช้งานที่มีสิทธิ์ระดับสูง พร้อมกำหนดรหัสผ่านให้มีความซับซ้อนและยากต่อการคาดเดา และควรกำหนดนโยบายรหัสผ่าน เช่น หลีกเลี่ยงการใช้รหัสผ่านซ้ำ กำหนดรายการรหัสผ่านต้องห้าม (Blacklist) และส่งเสริมการใช้เครื่องมือจัดการรหัสผ่าน (Password Manager)

๕. อัปเดตระบบปฏิบัติการ ซอฟต์แวร์ อุปกรณ์ และส่วนประกอบของระบบต่าง ๆ ให้เป็นปัจจุบันอยู่เสมอ โดยเฉพาะระบบที่เชื่อมต่อกับเครือข่ายภายนอก ระบบเว็บไซต์ ระบบจัดการเนื้อหา และซอฟต์แวร์ที่มีความเสี่ยงสูง

๖. ติดตั้งและปรับปรุงระบบป้องกันมัลแวร์ให้มีความทันสมัยอยู่เสมอ โดยเฉพาะการป้องกันมัลแวร์ที่มุ่งขโมยข้อมูลบัญชีผู้ใช้งาน ข้อมูลรับรองสำหรับเชื่อมต่อระบบ และข้อมูลสำคัญอื่นของหน่วยงาน

๗. ตรวจสอบอุปกรณ์ของผู้ใช้งาน โดยเฉพาะกรณีการปฏิบัติงานจากภายนอกหน่วยงาน อุปกรณ์ของผู้ดูแลระบบ และอุปกรณ์ที่ใช้เข้าถึงระบบสำคัญ เพื่อให้มั่นใจว่ามีมาตรการป้องกันที่เหมาะสม และไม่ตกอยู่ในภาวะเสี่ยงต่อการรั่วไหลของข้อมูล

๘. เฝ้าระวังและวิเคราะห์บันทึกการใช้งานระบบ (Log) อย่างต่อเนื่อง และนำข้อมูลที่เกี่ยวข้องกับภัยคุกคามมาใช้ในการตรวจจับและป้องกัน โดยเฉพาะความผิดปกติของการเข้าสู่ระบบ การเรียกใช้งานระบบจากตำแหน่งที่ไม่คุ้นเคย การใช้งานบัญชีสิทธิ์สูง และการเข้าถึงข้อมูลสำคัญที่ผิดไปจากปกติ

๙. ตรวจสอบและควบคุมการเข้าถึงของระบบหรือผู้ให้บริการภายนอกอย่างรัดกุม รวมถึงกำหนดสิทธิ์การเข้าถึงสำหรับระบบเชื่อมต่อ โปรแกรมประยุกต์ และ Application Programming Interface (API) ตามความจำเป็น จัดเก็บข้อมูลรับรอง กุญแจลับ และโทเคนสำหรับการเชื่อมต่ออย่างปลอดภัย และเฝ้าระวังการใช้งานที่ผิดปกติอย่างสม่ำเสมอ

๑๐. จัดให้มีระบบบริหารจัดการบัญชีผู้ใช้งานและสิทธิ์การเข้าถึงแบบรวมศูนย์ เพื่อควบคุมวงจรชีวิตบัญชีผู้ใช้งานอย่างเป็นระบบ ครอบคลุมการสร้าง การแก้ไข การระงับ และการยกเลิกบัญชี รวมถึงการเพิกถอนสิทธิ์ทันทีเมื่อมีการเปลี่ยนแปลงหน้าที่หรือพ้นสภาพการปฏิบัติงาน รวมถึงกำหนดกระบวนการยืนยันตัวตน (Identity Proofing) สำหรับการสร้างบัญชี การกู้คืนบัญชี และการเปลี่ยนแปลงข้อมูลสำคัญ เพื่อป้องกันการแอบอ้างตัวตน

๑๑. ควบคุมการกำหนดสิทธิ์การเข้าถึงตามหน้าที่และความจำเป็นของการปฏิบัติงาน พร้อมทบทวนสิทธิ์ของผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องภายนอกเป็นระยะ เพื่อลดความเสี่ยงจากการเข้าถึงข้อมูลหรือระบบเกินความจำเป็น รวมทั้งลดความเสี่ยงจากการใช้งานโดยไม่เหมาะสมจากบุคลากรภายใน

๑๒. กำหนดมาตรการป้องกันข้อมูลรั่วไหลอย่างเหมาะสม โดยจำแนกประเภทข้อมูลสำคัญ จำกัดการเข้าถึงตามระดับความจำเป็น เข้ารหัสข้อมูลทั้งขณะจัดเก็บและขณะรับส่ง และควบคุมการส่งออกข้อมูลผ่านระบบอีเมล เว็บแอปพลิเคชัน ระบบคลาวด์ และอุปกรณ์พกพา เพื่อป้องกันการนำข้อมูลออกจากระบบโดยไม่ได้รับอนุญาต รวมถึงควบคุมการใช้งานข้อมูลผ่านเว็บเบราว์เซอร์ และป้องกันการจัดเก็บข้อมูลรับรองในลักษณะที่ไม่ปลอดภัย

๑๓. จัดให้มีการทดสอบความมั่นคงปลอดภัยของระบบอย่างสม่ำเสมอ เช่น การประเมินช่องโหว่ การทดสอบเจาะระบบ และการตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ ระบบเชื่อมต่อ และบริการภายนอก เพื่อค้นหาและลดความเสี่ยงก่อนเกิดเหตุการณ์จริง รวมถึงกำหนดมาตรการควบคุมการใช้งาน session เช่น การกำหนดระยะเวลาหมดอายุของ session และการยกเลิก session เมื่อพบพฤติกรรมผิดปกติ

๑๔. สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้อง โดยให้ความรู้เกี่ยวกับการตั้งรหัสผ่านอย่างปลอดภัย การใช้งาน MFA การระวังภัยจากการหลอกลวงทางอิเล็กทรอนิกส์ การดูแลข้อมูลรับรองสำหรับเชื่อมต่อระบบ และแนวทางการปฏิบัติที่ปลอดภัยในการใช้งานระบบสารสนเทศของหน่วยงาน

๑๕. เมื่อพบหรือสงสัยว่ารหัสผ่านรั่วไหลให้แจ้งให้ผู้ใช้งานเปลี่ยนทันทีโดยใช้รหัสผ่านใหม่ที่ปลอดภัย ไม่ให้ใช้รหัสผ่านเดิม

แนวทางการตั้งและเปลี่ยนรหัสผ่านระบบ CYCL

1. หลักเกณฑ์การตั้งรหัสผ่านใหม่

รหัสผ่านใหม่ต้องมีความยาวอย่างน้อย 6 อักขระ ประกอบด้วยอักขระอย่างน้อย 2 ประเภท จากกลุ่มอักขระดังต่อไปนี้

1) ตัวอักษรภาษาอังกฤษตัวเล็ก (a-z)
2) ตัวอักษรภาษาอังกฤษตัวใหญ่ (A-Z)
3) ตัวเลข (0-9)
4) สัญลักษณ์พิเศษ (เช่น $, #, !, ?)

ตัวอย่างการตั้งรหัสผ่าน เพื่อให้ผู้ใช้งานสามารถกำหนดรหัสผ่านได้อย่างถูกต้อง ตัวอย่างรหัสผ่านที่เป็นไปตามหลักเกณฑ์ มีดังนี้

ตัวอย่างรหัสผ่าน	ประเภทอักขระที่ใช้
Cy3#26	ตัวพิมพ์ใหญ่, ตัวพิมพ์เล็ก, ตัวเลข, และสัญลักษณ์พิเศษ
YoutH9	ตัวพิมพ์ใหญ่, ตัวพิมพ์เล็ก, และตัวเลข
Dla@69	ตัวพิมพ์ใหญ่, ตัวพิมพ์เล็ก, ตัวเลข, และสัญลักษณ์พิเศษ
CYC2026!	ตัวพิมพ์ใหญ่, ตัวเลข และสัญลักษณ์พิเศษ

ตัวอย่างรหัสผ่านที่ไม่เหมาะสม เช่น 123456 หรือ abcdef เนื่องจากมีอักขระเพียงประเภทเดียว หรือเป็นรูปแบบที่สามารถคาดเดาได้ง่าย

หมายเหตุ : ตัวอย่างรหัสผ่านข้างต้นจัดทำขึ้นเพื่อประกอบความเข้าใจเท่านั้น ผู้ใช้งานควรกำหนดรหัสผ่านของตนเอง และไม่ควรนำตัวอย่างดังกล่าวไปใช้เป็นรหัสผ่านจริง

2. คำแนะนำและข้อควรระวังในการตั้งรหัสผ่าน

2.1 รูปแบบที่ไม่เหมาะสม (หลีกเลี่ยงการใช้งาน)

- วัน เดือน ปีเกิด
- หมายเลขบัตรประชาชน
- หมายเลขโทรศัพท์
- รหัสพนักงาน หรือลำดับตัวเลขเรียงกัน (เช่น 123456)
- ชื่อ-นามสกุล หรือข้อมูลส่วนตัวที่คาดเดาได้ง่ายจากสื่อสังคมออนไลน์

2.2 รูปแบบที่เหมาะสม (แนะนำให้ใช้งาน)

- สุ่มผสมตัวอักษรและตัวเลขที่ไม่เกี่ยวข้องกันโดยตรง (เช่น Cy3#26 หรือ YoutH9)
- หลีกเลี่ยงการใช้รหัสผ่านซ้ำกับระบบงานอื่น ๆ

3. ขั้นตอนการเปลี่ยนรหัสผ่านระบบ CYCL
   1) เข้าสู่เว็บไซต์ระบบ ที่ https://cycl.dla.go.th/pub/landing.do
   2) ดำเนินการลงชื่อเข้าใช้งาน (Log in) ตามปกติ
   3) ระบบจะแสดงหน้าจอให้ “เปลี่ยนรหัสผ่าน” โดยอัตโนมัติ
   4) ระบุ “รหัสผ่านเดิม” และกำหนด “รหัสผ่านใหม่” ให้เป็นไปตามเกณฑ์ที่กำหนด
   5) ตรวจสอบความถูกต้องและกดปุ่ม “บันทึก” เพื่อยืนยันการเปลี่ยนรหัสผ่าน

ขั้นตอนการเปลี่ยนรหัสผ่านระบบ CYCL

1. **การเข้าสู่ระบบ (Login)**

   1) ให้พิมพ์ https://cycl.dla.go.th/pub/landing.do ช่องแสดง URL Address

   2) คลิกที่เมนู เข้าสู่ระบบ

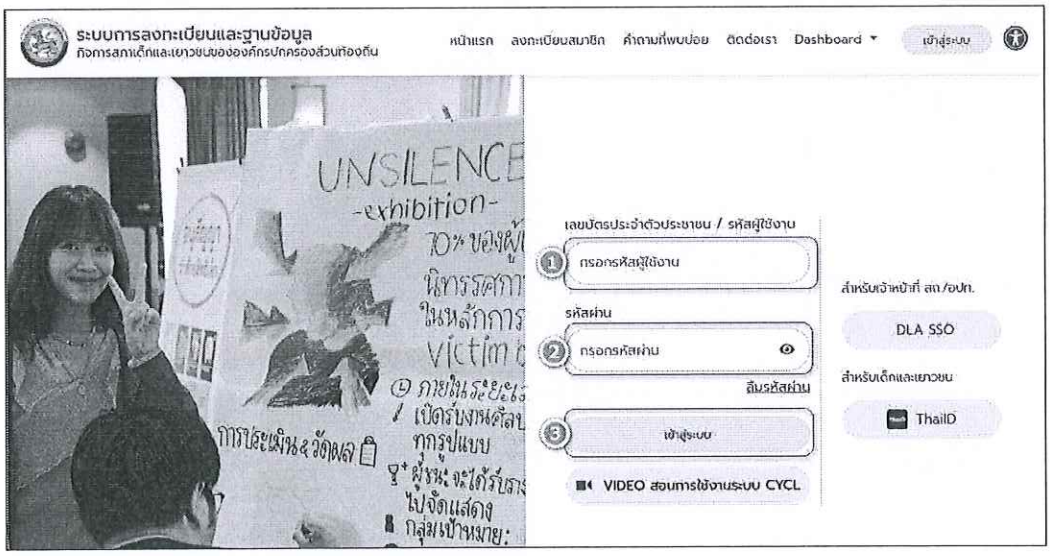
รูปภาพที่ 1 หน้าจอการเข้าสู่ระบบ (Login)

1.1 เข้าสู่ระบบด้วย ชื่อผู้ใช้งานและรหัสผ่าน

1) กรอกรหัสผู้ใช้งาน

2) กรอกรหัสผ่าน

3) คลิกปุ่ม เข้าสู่ระบบ ระบบจะแสดงหน้าจอให้ “เปลี่ยนรหัสผ่าน” โดยอัตโนมัติ



รูปภาพที่ 2 หน้าจอเข้าสู่ระบบด้วย ชื่อผู้ใช้งานและรหัสผ่าน

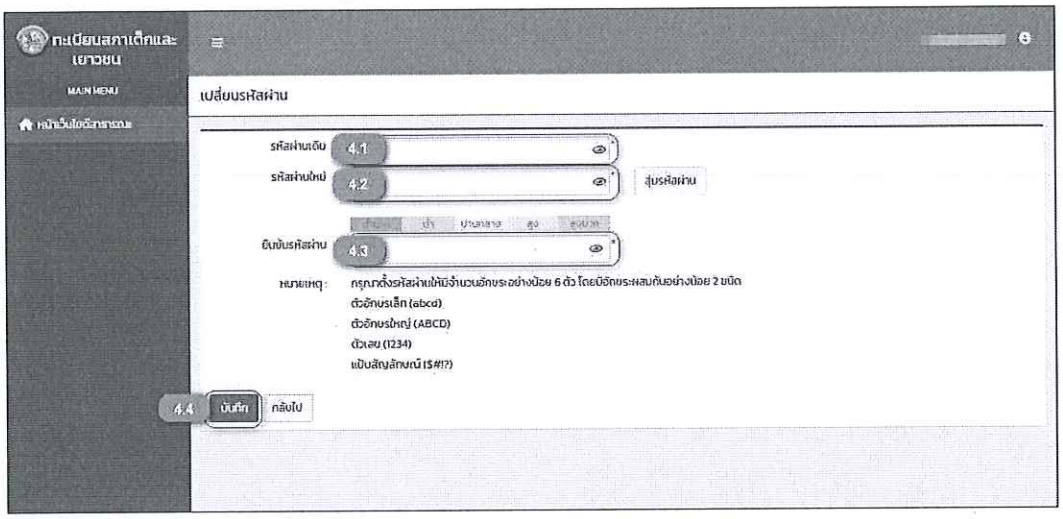
4) กรณี เลือกกำหนดรหัสผ่านเอง

(4.1) กรอกรหัสผ่านเดิม

(4.2) กรอกรหัสผ่านใหม่

(4.3) กรอกยืนยันรหัสผ่าน

(4.4) ตรวจสอบความถูกต้อง และคลิกปุ่ม บันทึก เพื่อยืนยันการเปลี่ยนรหัสผ่าน



รูปภาพที่ 3 หน้าจอ“เปลี่ยนรหัสผ่าน” กรณี เลือกกำหนดรหัสผ่านเอง

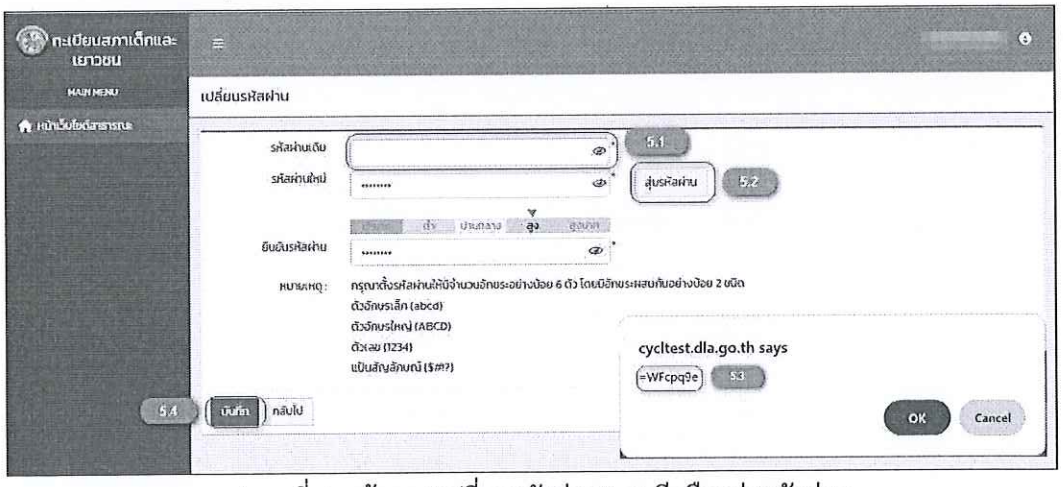
5) กรณี เลือกสุ่มรหัสผ่าน

(5.1) กรอกรหัสผ่านเดิม

(5.2) คลิกที่ปุ่ม สุ่มรหัสผ่าน

(5.3) ระบบจะแสดง Pop-up รหัสผ่านขึ้นมา ให้ผู้ใช้งาน คัดลอกและจัดเก็บรหัสผ่านไว้สำหรับใช้ในการเข้าสู่ระบบ

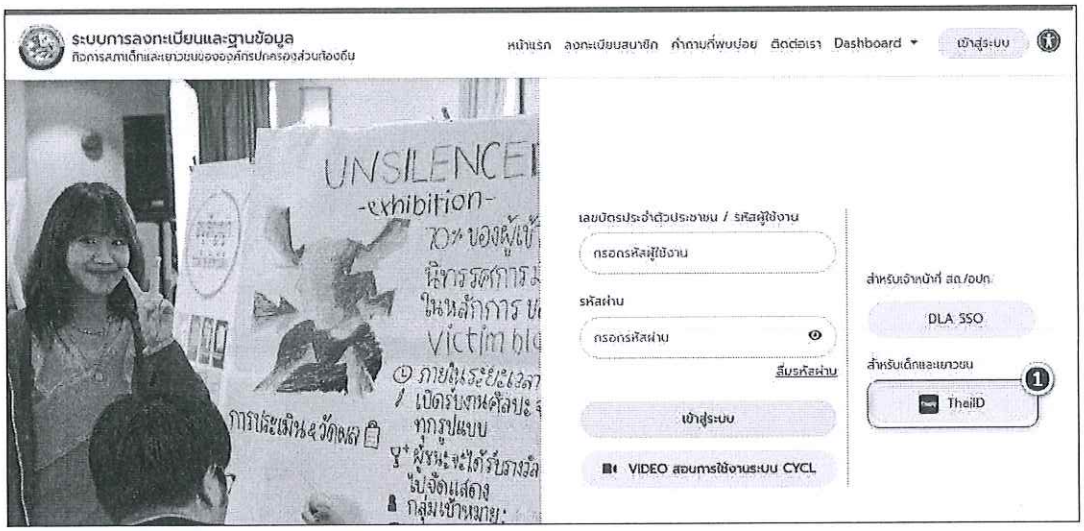
(5.4) คลิกปุ่ม บันทึก



รูปภาพที่ 4 หน้าจอ “เปลี่ยนรหัสผ่าน” กรณี เลือกสุ่มรหัสผ่าน

1.2 เข้าสู่ระบบด้วย ThaiD

1) คลิกปุ่ม ThaiID



รูปภาพที่ 5 หน้าจอเข้าสู่ระบบด้วย ThaiD

2) ระบบจะแสดง QR Code เพื่อสแกนด้วยแอปพลิเคชัน ThaiD

รูปภาพที่ 6 QR Code เพื่อสแกนด้วยแอปพลิเคชัน ThaiD

3) เปิดแอป ThaiD บนอุปกรณ์ของผู้ใช้งาน แล้วสแกน QR Code ที่ปรากฏ เมื่อการสแกนสำเร็จ ระบบจะแสดงหน้าจอให้ “เปลี่ยนรหัสผ่าน” โดยอัตโนมัติ

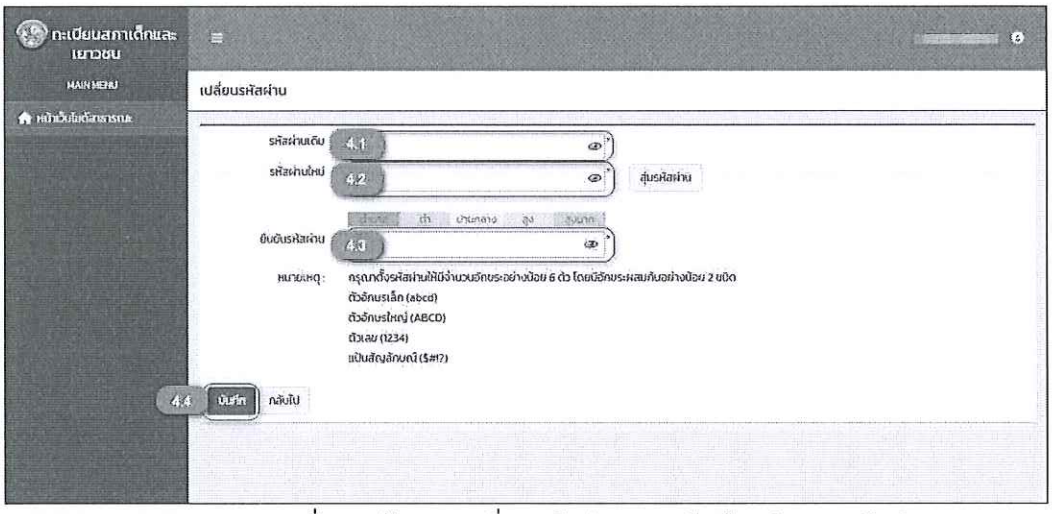
4) กรณี เลือกกำหนดรหัสผ่านเอง

(4.1) กรอกรหัสผ่านเดิม

(4.2) กรอกรหัสผ่านใหม่

(4.3) กรอกยืนยันรหัสผ่าน

(4.4) ตรวจสอบความถูกต้อง และคลิกปุ่ม บันทึก เพื่อยืนยันการเปลี่ยนรหัสผ่าน



รูปภาพที่ 7 หน้าจอ “เปลี่ยนรหัสผ่าน” กรณี เลือกกำหนดรหัสผ่านเอง

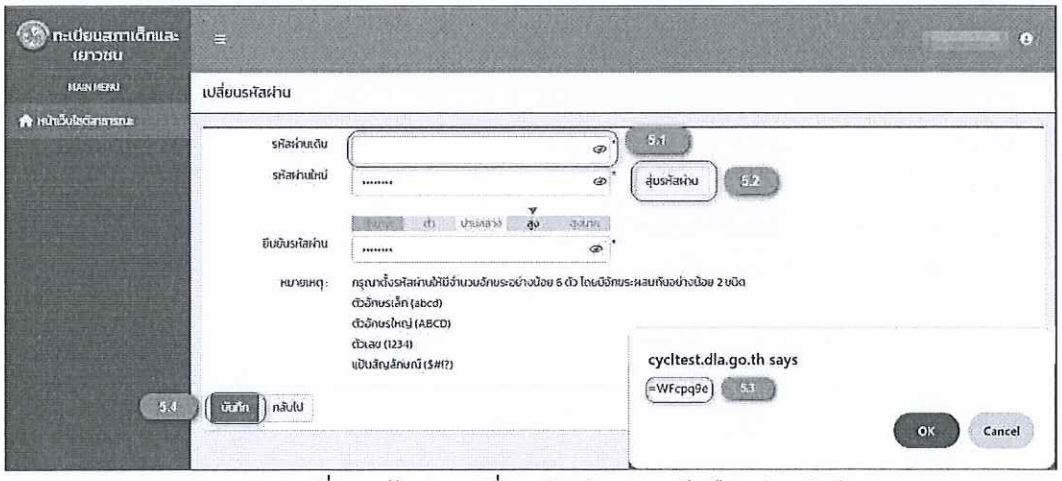
5) กรณี เลือกสุ่มรหัสผ่าน

(5.1) กรอกรหัสผ่านเดิม

(5.2) คลิกที่ปุ่ม สุ่มรหัสผ่าน

(5.3) ระบบจะแสดง Pop-up รหัสผ่านขึ้นมา ให้ผู้ใช้งาน คัดลอกและจัดเก็บรหัสผ่านไว้สำหรับใช้ในการเข้าสู่ระบบ

(5.4) คลิกปุ่ม บันทึก



รูปภาพที่ 8 หน้าจอ “เปลี่ยนรหัสผ่าน” กรณี เลือกสุ่มรหัสผ่าน