

เรื่องพิจารณาให้ความเห็นชอบ

โครงการจัดซื้อระบบยืนยันตัวตนแบบหลายปัจจัย (Multifactor Authentication)

วงเงินรวมทั้งสิ้น 34,443,300.00 บาท (รวมภาษีมูลค่าเพิ่ม 7%)

ตามข้อสังเกตของคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ ของกระทรวงมหาดไทย ครั้งที่ 4/2565 วันที่ 11 สิงหาคม 2565

ข้อสังเกตและข้อเสนอแนะของคณะกรรมการฯ

- คณะกรรมการมีข้อสังเกตและข้อเสนอแนะสรุปได้ ดังนี้
- โครงการนี้เป็นการอำนวยความสะดวกให้กับบุคลากรในหน่วยงาน
 - โครงการดังกล่าวควรจัดทำ cost benefit หลายๆด้าน เช่นมูลค่าต่อการเสียหายในการโดนโจมตีทางไซเบอร์ในแต่ละครั้ง หรือด้านอื่นๆที่สามารถคำนวณได้เพื่อประกอบการพิจารณา
 - ระบบในโครงการมีสิทธิผู้ใช้งานจำนวน ๓๐,๐๐๐ ผู้ใช้งานซึ่งมีจำนวนมาก หน่วยงานควรกำหนดเฉพาะบุคลากรที่จำเป็นต้องใช้งานเพื่อความคุ้มค่าในการใช้งบประมาณ
 - โครงการที่ผู้แทนเปรียบเทียบหรือหาข้อมูลมานั้นไม่เพียงพอต่อการพิจารณาเนื่องจากไม่มีคุณสมบัติขั้นต้นของหน่วยงาน รวมถึงจำนวนที่หน่วยงานที่หน่วยงานจัดหามีจำนวนน้อยกว่าจึงอาจทำให้ราคาสูงกว่า
 - หน่วยงานควรแยกระบบและตัวบุคคลโดยจัดลำดับความสำคัญเพื่อมาวิเคราะห์ความสำคัญต่อการใช้ระบบเพื่อประกอบการพิจารณา
 - ระบบ PEA E-mail ที่หน่วยงานเลือกใช้น่าจะมีระบบป้องกันอยู่แล้วซึ่งไม่จำเป็นต้องใช้ระบบป้องกันเพิ่มเติม
 - หน่วยงานควรพิจารณาการป้องกันภัยทางไซเบอร์ด้วยวิธีอื่นประกอบเพิ่มเติมเพื่อช่วยในการป้องกัน เช่น การประกาศข้อควรระวังการใช้งาน การอบรมการใช้งานให้กับพนักงาน การจำกัดการใช้งานสำหรับพนักงานจ้างเหมาบริการ เป็นต้น

มติที่ประชุม ให้ทบทวนและปรับแก้ไขเอกสารตามข้อสังเกตและข้อเสนอแนะของคณะกรรมการฯ พร้อมลงนามกำกับเอกสารทุกหน้า ส่งให้คณะทำงานฯ ตรวจสอบก่อนนำเสนอที่ประชุมคณะกรรมการเพื่อพิจารณาต่อไป

ตามข้อสังเกตของคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ ของกระทรวงมหาดไทย ครั้งที่ 4/2565 วันที่ 11 สิงหาคม 2565

1. โครงการนี้เป็นการอำนวยความสะดวกให้กับบุคลากรในหน่วยงาน

กฟภ. มีวัตถุประสงค์เพื่อปรับเปลี่ยนให้ กฟภ. สู่ Digital Utility ภายในปี 2565 ตามทิศทางและตำแหน่งยุทธศาสตร์ที่กำหนดไว้ในแผนยุทธศาสตร์ กฟภ. พ.ศ. 2564 – 2568 ซึ่งสอดคล้องกับ นโยบายภาครัฐ และนโยบายภาคพลังงาน ซึ่ง กฟภ.จะเป็นส่วนหนึ่งในการช่วยขับเคลื่อนภาคเศรษฐกิจและสังคมของประเทศภายใต้แนวคิด และการปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัลตามแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย โดยการสร้างมาตรฐานงานบริการที่เป็นเลิศ และพัฒนาระบบไฟฟ้าให้ทันสมัยมั่นคง เชื่อถือได้ เพื่อตอบสนอง ความต้องการของผู้ใช้ไฟฟ้าได้อย่างรวดเร็ว มีประสิทธิภาพ อีกทั้ง ระบบงานเป็นลักษณะ Application ซึ่งมุ่งเน้นให้พนักงานทำงานได้ Anywhere Anytime ด้วยเทคโนโลยีปัจจุบัน การใช้เพียง username/password ไม่เพียงพอ จึงจำเป็นต้องมีการยืนยันตัวตนมากกว่า 1 ปัจจัย

วัตถุประสงค์เน้นป้องกันข้อมูลของบุคลากรภายในองค์กร

- เพื่อป้องกันอาชญากรไซเบอร์โจรกรรมข้อมูลผู้ใช้งาน และนำไปใช้สร้างความเสียหายต่อระบบสารสนเทศ
- เพื่อพิสูจน์ตัวตนของผู้เข้าใช้ระบบสารสนเทศว่าเป็นเจ้าของบัญชีตัวจริง
- เพื่อป้องกันข้อมูลส่วนบุคคลของบุคลากรภายในองค์กร

ตามข้อสังเกตของคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ ของกระทรวงมหาดไทย ครั้งที่ 4/2565 วันที่ 11 สิงหาคม 2565

2. โครงการดังกล่าวควรจัดทำ cost benefit หลายๆด้าน เช่นมูลค่าต่อการเสียหายในการโจมตีทางไซเบอร์ในแต่ละครั้ง หรือด้านอื่นๆที่สามารถคำนวณได้เพื่อประกอบการพิจารณา

ความคุ้มค่าโครงการ : ผลตอบแทนที่ไม่เป็นตัวเงิน

- ลดความเสี่ยงจากการโจมตีทาง Cyber
- ป้องกันการสูญเสียชีวิต
- ยกกระดับมาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูลให้มีความปลอดภัยยิ่งขึ้น
- ลดผลกระทบต่อภาพลักษณ์ และชื่อเสียงของ กฟผ.
- ลดการละเมิดทางกฎหมายที่เกี่ยวข้องกับ พรบ.ข้อมูลส่วนบุคคล (PDPA)

ผู้เกี่ยวข้องหลัก (Key Stakeholders) : ทุกหน่วยงาน ภายใน กฟผ.

ตามข้อสังเกตของคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ ของกระทรวงมหาดไทย ครั้งที่ 4/2565 วันที่ 11 สิงหาคม 2565

3. ระบบในโครงการมีสิทธิผู้ใช้งานจำนวน 30,000 ผู้ใช้งานซึ่งมีจำนวนมาก หน่วยงานควรกำหนดเฉพาะบุคลากรที่จำเป็นต้องใช้งานเพื่อความคุ้มค่าในการใช้งบประมาณ และ 5. หน่วยงานควรแยกระบบและตัวบุคคลโดยจัดลำดับความสำคัญเพื่อมาวิเคราะห์ความสำคัญ ต่อการใช้ระบบเพื่อประกอบการพิจารณา

เนื่องจากระบบงานสารสนเทศของ กฟภ. ได้เปิดให้บริการกับบุคลากรทุกคน โดยได้มีการจัดความสำคัญระบบและกลุ่มผู้ใช้งานเพื่อเข้าระบบแล้ว จึงจำเป็นต้องจัดซื้อให้ครอบคลุมกับจำนวนผู้ใช้งาน

- ระบบ Virtual Private Network (VPN) ผู้ใช้งาน 30,000 user รองรับการทำงาน Work Form Home
- ระบบ Virtual Desktop Infrastructure (VDI) ผู้ใช้งาน 30,000 user (concurrent 4,000 user)
- ระบบ PEA-email (Microsoft Exchange Outlook Web App : OWA) ผู้ใช้งาน 30,000 user
- ระบบ Privileged Access Management (PAM) ผู้ใช้งาน 100 user (Admin)
- ระบบ PEA Work D ผู้ใช้งาน 13,000 user ระบบงาน การก่อสร้าง-การบำรุงรักษา-การปฏิบัติงาน ที่เกี่ยวข้องกับงานบริการผู้ใช้ไฟ
- ระบบ PEA Life ผู้ใช้งาน 30,000 user

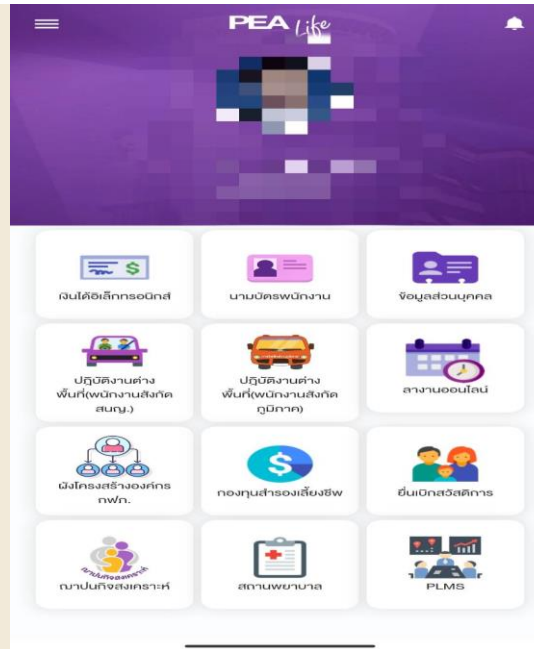
ตามข้อสังเกตของคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ ของกระทรวงมหาดไทย ครั้งที่ 4/2565 วันที่ 11 สิงหาคม 2565

3. ระบบในโครงการมีสิทธิผู้ใช้งานจำนวน 30,000 ผู้ใช้งานซึ่งมีจำนวนมาก หน่วยงานควรกำหนดเฉพาะบุคลากรที่จำเป็นต้องใช้งานเพื่อความคุ้มค่าในการใช้งบประมาณ

ระบบ PEA Life ผู้ใช้งาน 30,000 user

(ระบบบริหารจัดการของพนักงาน)

- ข้อมูลเงินเดือนของพนักงาน
- ข้อมูลส่วนบุคคลของพนักงาน
- การปฏิบัติงานต่างจังหวัดของพนักงาน
- ประวัติการรักษาพยาบาล
- การยื่นเบิกสวัสดิการต่างๆ ของพนักงาน
- การลางานออนไลน์
- กองทุนสำรองเลี้ยงชีพ



ตามข้อสั่งเกตของคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ ของกระทรวงมหาดไทย ครั้งที่ 4/2565 วันที่ 11 สิงหาคม 2565

PEA Work D

ระบบ PEA Work D ผู้ใช้งาน 13,000 user

ประเภทงานทั่วไป (Manage D)

- ระบบติดตามการเบิกจ่ายงบลงทุน (CAPEX-ex)
- ระบบบริหารจัดการยานพาหนะของ กฟภ. (VMS)
- ระบบลงนามเอกสารด้วยลายเซ็นดิจิทัล (DigiSign)

ประเภทออกแบบและงานวางแผน (Plan D)

- ระบบบริหารโครงการขนาดใหญ่ Capital Project Management (CPM)
- ระบบขึ้นทะเบียนอุปกรณ์สถานีไฟฟ้า (Product Lists)
- ระบบงานออกแบบและประมาณการงานก่อสร้างสถานีไฟฟ้า

ประเภทงานก่อสร้าง (Construct D)

- ระบบคำนวณโมเมนต์ที่เกิดขึ้นกับเสาไฟฟ้า (Happy Pole)
- ระบบจัดการคำขอรับบริการทางอิเล็กทรอนิกส์สำหรับงานก่อสร้างและบริหารโครงการ กฟภ. (eR-CON)

ประเภทงานบำรุงรักษา (Maintain D)

- ระบบตรวจนับหม้อแปลงคงคลัง (BatchR Monitor)
- ระบบบริหารจัดการงานบำรุงรักษาหม้อแปลงในระบบจำหน่ายของ กฟภ. (Bisme)
- ระบบตรวจสอบความปลอดภัยสำหรับการปฏิบัติงานในระบบไฟฟ้า (WeSafe)
- ระบบจัดการคำขอรับบริการทางอิเล็กทรอนิกส์สำหรับงานบำรุงรักษาระบบไฟฟ้า กฟภ. (eR-MTN)
- ระบบมอบหมายและติดตามงานสำหรับงานบำรุงรักษาระบบ

ประเภทงานปฏิบัติการ (Operate D)

- ระบบวิเคราะห์แรงดันตกด้วยอุปกรณ์ VloT
- ระบบจัดการคำขอรับบริการทางอิเล็กทรอนิกส์สำหรับงานปฏิบัติการ กฟภ. (eR-OPS)
- ระบบแก้ไขปัญหาไฟฟ้าขัดข้องอัจฉริยะแบบเคลื่อนที่ (MWM)

ประเภทงานบริการลูกค้า (Service D)

- ระบบติดตามข้อตกลงระดับการให้บริการ (SLA Tracking System)
- ระบบติดตามสถานะหนี้ผู้ใช้ไฟรายย่อย (Bill Tracking)
- ระบบบริหารงานบริการลูกค้า (WOM)

สนับสนุนการวางแผน การก่อสร้าง-การบำรุงรักษา-การปฏิบัติงาน
และงานบริการลูกค้าของ กฟภ.

ตามข้อสังเกตของคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ ของกระทรวงมหาดไทย ครั้งที่ 4/2565 วันที่ 11 สิงหาคม 2565

4. โครงการที่ผู้แทนเปรียบเทียบหรือหาข้อมูลมานั้นไม่เพียงพอต่อการพิจารณาเนื่องจากไม่มีคุณสมบัติขั้นต้นของหน่วยงาน รวมถึงจำนวนที่หน่วยงานจัดหามีจำนวนน้อยกว่าจึงอาจทำให้ราคาสูงกว่า

เนื่องจากข้อมูลที่ได้มาเป็นข้อมูลที่ปรากฏบน Internet จึงไม่มีรายละเอียดของคุณลักษณะเฉพาะที่ครอบคลุมการดำเนินงานของหน่วยงานนั้น อีกทั้งเป็นข้อมูลภายในองค์กรนั้นๆ ที่ไม่อาจเปิดเผย

ในการจัดหาครั้งนี้ กฟภ.ได้ราคาต่อหน่วยที่ถูกกว่า โดยมีการสืบราคาดังนี้

- จากท้องตลาด 3 ราย (บริษัท สเตป โซลูชันส์ จำกัด, บริษัท อี.เอ็น. ซีอาร์ท จำกัด (มหาชน), บริษัท ไอ ทู เอ็นเตอร์ไพรส์ จำกัด)
- เทียบราคาจากหน่วยงานที่เคยจัดซื้อ (SCB, UOB, GSB)

ตามข้อสังเกตของคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ ของกระทรวงมหาดไทย ครั้งที่ 4/2565 วันที่ 11 สิงหาคม 2565

6. ระบบ PEA E-mail ที่หน่วยงานเลือกใช้น่าจะมีระบบป้องกันอยู่แล้วซึ่งไม่จำเป็นต้องใช้ระบบป้องกันเพิ่มเติม

PEA E-mail ของ กฟภ. เป็น On Premise ไม่สามารถ Enable MFA ต้องซื้อสิทธิ์เพิ่มจาก On Cloud

Feature	Azure AD Free - Security defaults (enabled for all users)	Azure AD Free - Global Administrators only	Office 365	Azure AD Premium P1	Azure AD Premium P2
Protect Azure AD tenant admin accounts with MFA	•	• (Azure AD Global Administrator accounts only)	•	•	•
Mobile app as a second factor	•	•	•	•	•
Phone call as a second factor		•	•	•	•
SMS as a second factor		•	•	•	•
Admin control over verification methods		•	•	•	•
Fraud alert				•	•
MFA Reports				•	•
Custom greetings for phone calls				•	•
Custom caller ID for phone calls				•	•
Trusted IPs				•	•
Remember MFA for trusted devices		•	•	•	•
MFA for on-premises applications				•	•
Conditional access				•	•

Premium P1

Designed to empower organizations with more demanding identity and access management needs, Azure Active Directory Premium edition adds feature-rich enterprise-level identity management capabilities and enables hybrid users to seamlessly access on-premises and cloud capabilities. This edition includes everything you need for information worker and identity administrators in hybrid environments across application access, self-service identity and access management (IAM), and security in the cloud.

Premium P2

Azure Active Directory Premium P2 includes every feature of all other Azure Active Directory editions enhanced with advanced identity protection and privileged identity management capabilities.

Feature comparisons for each tier located on [Active Directory documentation](#).

Purchase Method	Azure Premium P1	Azure Premium P2
Microsoft Representative	Included with Microsoft 365	Included with Microsoft 365
Online	\$6 user/month*	\$9 user/month*

* Annual commitment

$30,000 * 6\$ * 36 = 6,480,000\$$ ประมาณ 230,752,800 บาท (1\$ = 35.61 บาท)

ตามข้อสังเกตของคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ ของกระทรวงมหาดไทย ครั้งที่ 4/2565 วันที่ 11 สิงหาคม 2565

7. หน่วยงานควรพิจารณาการป้องกันภัยทางไซเบอร์ด้วยวิธีอื่นประกอบเพิ่มเติมเพื่อช่วยในการป้องกัน เช่น การประกาศข้อควรระวังการใช้งาน การอบรมการใช้งานให้กับพนักงาน การจำกัดการใช้งานสำหรับพนักงานจ้างเหมาบริการ เป็นต้น

มาตรการการใช้ทรัพยากรสารสนเทศ ของ กฟผ. พ.ศ. 2563

3 ห้าม **7 ใ้**

- ห้ามการนำเครื่องคอมพิวเตอร์เคลื่อนที่เข้าใช้ กฟผ. จัดฯ ให้
- ห้ามใช้คอมพิวเตอร์ที่นำเข้ามาจากต่างประเทศ หรือใช้คอมพิวเตอร์ที่นำเข้ามาจากนอกที่อื่นของ กฟผ. ให้ใช้ภายใน
- ห้ามนำหรือถอดวงจรร่วมกันด้วยเครื่องคอมพิวเตอร์ของ กฟผ. หากมีความจำเป็น ต้องขออนุญาตจากฝ่ายไอทีของ กฟผ.

ภาพนิยามสัญลักษณ์ของ กฟผ. อาศัยในปฏิทินราชการของผู้มีอำนาจและบุคลากรที่มีอยู่ 3 และอาจมีในเอกสารสื่อที่เกี่ยวข้องกับ กฟผ. หรือเผยแพร่ในสื่อสาธารณะบนช่องทางอื่นและสื่อออนไลน์และสื่อของ กฟผ.

ห้ามใช้คอมพิวเตอร์ส่วนบุคคล (Personal) และใส่พาสเวิร์ด (Password) ของตนเองที่อื่นตามนี้

ติดตั้ง Anti-Virus หรือซอฟต์แวร์ที่ช่วยป้องกันการโจมตี กฟผ. กำหนด

ใช้ระบบปฏิบัติการและซอฟต์แวร์ที่มีลิขสิทธิ์ (License) ถูกต้อง

ใช้ท่าเฉพาะการใช้งานกรณีใช้งานเครื่องคอมพิวเตอร์ที่อื่น

ใช้รหัสผ่านสารสนเทศตามปฏิทินของ กฟผ. กำหนด


ใส่สายป้องกันสายสัญญาณเช่นสาย ไรต์เทคที่มีเครื่องหมายการค้า กฟผ. กำหนด

ใช้ Email ของ กฟผ. ในการทำงานเท่านั้น และห้ามนำไปใช้ส่วนตัว

ห้ามดาวน์โหลดซอฟต์แวร์ของ กฟผ. อาศัยในปฏิทินราชการของผู้มีอำนาจและบุคลากรที่มีอยู่ 3 และอาจมีในเอกสารสื่อที่เกี่ยวข้องกับ กฟผ. หรือเผยแพร่ในสื่อสาธารณะบนช่องทางอื่นและสื่อออนไลน์และสื่อของ กฟผ.

ห้ามดาวน์โหลดซอฟต์แวร์ของ กฟผ. อาศัยในปฏิทินราชการของผู้มีอำนาจและบุคลากรที่มีอยู่ 3 และอาจมีในเอกสารสื่อที่เกี่ยวข้องกับ กฟผ. หรือเผยแพร่ในสื่อสาธารณะบนช่องทางอื่นและสื่อออนไลน์และสื่อของ กฟผ.

- ระเบียบการไฟฟ้าส่วนภูมิภาคว่าด้วยการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2560
- นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. 2561
- นโยบายความมั่นคงปลอดภัยสารสนเทศ (ฉบับที่2) พ.ศ. 2562
- แนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. 2562
- มาตรการการใช้งานทรัพยากรสารสนเทศ



การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

แนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ
ประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๒

(กรณีศึกษาที่หน่วยงานใด)

แผนการอบรมพนักงาน

ตารางสรุปแผนฝึกอบรมและพัฒนาบุคลากร ประจำปี 2565
ตาม Core Competency Managerial Competency ยุทธศาสตร์ แผนงานต่างๆ ซึ่งกฎหมาย ระเบียบกติกาคณะ
บุคลากร และความรู้เฉพาะทาง

ที่	หลักสูตร	กลุ่มเป้าหมาย	ระยะเวลา (วัน)	จำนวนผู้	จำนวนคนต่อวัน	จำนวน ทั้งหมด
104	Change Influencer	ผู้บริหารและพนักงานที่ดำเนินการทำ โครงการ Change Leader Program ปี 2564 และนักพัฒนา บุคคลต้นแบบ	7	1	10	10
105	Change Leadership Program	ผู้บริหารระดับกลาง	7	3	25	75
รวมจำนวนผู้เข้าอบรม (รวม 6 หลักสูตร)						2085
7) ด้าน Digital						
106	ความตระหนักด้านความมั่นคงปลอดภัย สารสนเทศ สำหรับผู้พัฒนาระบบสารสนเทศ (Developer)	พนักงานปฏิบัติการพัฒนา ระบบฯ และออกแบบระบบสารสนเทศ จาก กศ. 12 ชม และ สกย.	16	1	100	100
107	ความตระหนักด้านความมั่นคงปลอดภัย สารสนเทศ สำหรับพนักงาน	พนักงานและผู้ช่วยของ กศก.	1	1	1000	1,000
108	ความตระหนักด้านความมั่นคงปลอดภัย สารสนเทศ สำหรับผู้บริหาร	ผู้บริหารระดับสูง และ กศก. 12 ชม	3	1	140	140
109	การตรวจประเมิน เชิงป้องกันของระบบสารสนเทศ Security Management System	พนักงานที่ปฏิบัติงานในระบบ สารสนเทศ ตามมาตรฐาน ISO/IEC 27001	2	1	50	50
110	การประเมินความ ปลอดภัยของระบบสารสนเทศ	พนักงานที่ปฏิบัติงานในระบบ สารสนเทศ ตามมาตรฐาน ISO/IEC 27001	2	1	50	50
111	ComplIA Security	พนักงาน จาก กศก. 12 ชม และ สกย.	5	1	30	30
112	การวิเคราะห์ข้อมูล	พนักงาน และผู้ช่วย กศก.	60			1,000
113	การนำข้อมูลไป ใช้ประโยชน์	พนักงานและผู้ช่วย กศก. และพนักงานที่เกี่ยวข้องกับ งานด้านเทคโนโลยีสารสนเทศ กศก. 12 ชม และ สกย.	2	1	50	50

7) ด้าน Digital

106	ความตระหนักด้านความมั่นคงปลอดภัย สารสนเทศ สำหรับผู้พัฒนาระบบสารสนเทศ (Developer)
107	ความตระหนักด้านความมั่นคงปลอดภัย สารสนเทศ สำหรับพนักงาน
108	ความตระหนักด้านความมั่นคงปลอดภัย สารสนเทศ สำหรับผู้บริหารด้านเทคโนโลยีดิจิทัล

การสื่อสารผ่าน Lockscreen และช่องทางอื่นๆ



STEP แรก
ของความปลอดภัยยุคดิจิทัล

กดปุ่ม **หรือ "L"**
เพื่อล็อกหน้าจอทุกครั้งก่อนลุกออกจากโต๊ะ

ล็อค แล้ว Lock

- ป้องกันไม่ให้บุคคลอื่นสอดส่อง
- หมดปัญหาการบันทึกข้อมูล
- ไฟล์งานที่ทำการไว้ยังอยู่ครบ
- ใช้ได้ทั้ง PC / Notebook

สร้างความปลอดภัยง่ายๆ ให้งานของเรา

สอบถามและรับทราบรายละเอียดได้ที่ฝ่าย IT Security
ข้อมูลภายใน <http://intranet.pea.co.th/content/cyber-security>



เนียนแค่ไหนไม่รู้เท่ากัน!!

สารพัดวิธีจับโป๊ะ: Phishing Mail

- ตรวจสอบที่มาของอีเมล**
เช็คตัวเลขก่อนกดตอบอีเมล
เพราะมีอาจมีพิกัดอีเมลปลอม
ที่คล้ายของจริงมาก
- สังเกตเนื้อหาอีเมลให้ดี**
Phishing Mail ปรกติไม่น่าสนใจแต่
มีอยู่ เร่งรัดให้รีบทำทันทีเมื่อแจ้ง
รวมตัวให้รีบตอบกลับด่วน
- ระวังลิงก์ที่มากับอีเมล**
ตรวจสอบแต่ละคอมโพส URL ของลิงก์ให้ดี
อย่าหลงกดไปเผลอคลิกเด็ดขาด
- ระวังไฟล์แนบอีเมล**
ไม่ควรถูกเปิดไฟล์แนบที่ส่งมาจากอีเมลที่ผู้รับ
เช่น ไฟล์นามสกุล exe bat cmd zip

สอบถามและรับทราบรายละเอียดได้ที่ฝ่าย IT Security
ข้อมูลภายใน <http://intranet.pea.co.th/content/cyber-security>