แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลจากการปฏิบัติงานที่บ้านของประเทศฟิลิปปินส์ (Protecting Personal Data in a Work From Home Arrangement) *

*ปิยะขวัญ ชมชื่น***

บทนำ

การแพร่ระบาดของ COVID - ๑๙ ส่งผลให้ประชาชนต้องปรับเปลี่ยนพฤติกรรมเพื่อรักษาระยะห่างทางกายภาพ (Physical Distancing) ข้อมูล ณ วันที่ ๒๗ พฤษภาคม พ.ศ. ๒๕๖๓ ประเทศฟิลิปปินส์พบผู้ป่วยยืนยันจำนวน ๑๔,๖๖๙ ราย เสียชีวิต ๘๘๖ ราย[๑] ก่อนหน้านี้ฟิลิปปินส์ได้ประกาศภาวะฉุกเฉินและใช้บังคับกฎหมาย Bayanihan To Heal As One ที่ให้อำนาจพิเศษแก่ประธานาธิบดีในการบริหารจัดการประเทศในช่วงสถานการณ์การแพร่ระบาดของ COVID – ๑๙ การดำเนินการต่าง ๆ ของฟิลิปปินส์อยู่ภายใต้มาตรการ lock-down ซึ่งหนึ่งในแนวปฏิบัติที่สำคัญคือการลดการเดินทางของประชาชนเพื่อลดความเสี่ยงในการแพร่กระจายของเชื้อ ในด้านของกิจกรรมการปฏิบัติงาน องค์กรภาครัฐและเอกชนจึงใช้รูปแบบการดำเนินงานโดยการจัดให้บุคคลากรปฏิบัติงานจากที่บ้าน (Work From Home) เพื่อรักษาสมดุลระหว่างการรักษาความปลอดภัยด้านสาธารณสุขของบุคคลากรที่ต้องเดินทางมาปฏิบัติงานและเพื่อให้การปฏิบัติงานขององค์กรสามารถดำเนินต่อไปได้ในภาวะวิกฤตอย่างไม่ติดขัด อย่างไรก็ดี การใช้มาตรการ Work From Home ในสภาวะการแพร่ระบาดของ COVID - ๑๙ นี้ สิ่งสำคัญที่องค์กรจำเป็นต้องคำนึงถึงคือเรื่องของการคุ้มครองข้อมูลขององค์กร วิธีการจัดการเอกสารและการเข้าถึงเอกสารที่มีข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต เนื่องจากอุปกรณ์ที่ใช้ในการปฏิบัติงานที่บ้านอาจไม่ได้รับการป้องกันที่เหมาะสมเพียงพอ เช่นนี้แล้ว เมื่อวันที่ ๑๕ พฤษภาคม พ.ศ. ๒๕๖๓ คณะกรรมการข้อมูลส่วนบุคคลของฟิลิปปินส์ (National Privacy Commission – NPC) ได้ออกประกาศชื่อ NPC PHE Bulletin No.12: Protecting Personal Data in a Work From Home Arrangement[๒] เพื่อให้คำแนะนำแก่องค์กรที่มีการจัดให้บุคคลากรปฏิบัติงานที่บ้านและการปฏิบัติงานรูปแบบอื่นที่ใช้เทคโนโลยีสารสนเทศ โดยแนวปฏิบัติดังกล่าวครอบคลุมถึงการคุ้มครองข้อมูลส่วนบุคคล มาตรการรักษาความปลอดภัยของข้อมูลโดยทั่วไป และการรักษาความปลอดภัยของข้อมูลสำหรับบุคคลากรที่ปฏิบัติงานที่บ้าน โดยมีสาระสำคัญ ดังนี้

<u>ด้านระบบและอุปกรณ์คอมพิวเตอร์</u>

๑. เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (Computers and other ICT peripherals)

องค์กรควรจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่เหมาะสม เพียงพอต่อการปฏิบัติงานของบุคคลากร กรณีที่องค์กรไม่สามารถจัดหาอุปกรณ์ได้เพียงพอและจำเป็นต้องให้ใช้อุปกรณ์ส่วนบุคคลที่

---

* บทความนี้เผยแพร่เมื่อวันที่ ๒๙ พฤษภาคม พ.ศ.๒๕๖๓ (ฉบับร่าง)

** บุคคลากรจัดทำข้อมูลกฎหมาย ฝ่ายอาเซียนและกิจการต่างประเทศ สำนักงานคณะกรรมการกฤษฎีกา

[๑] ข้อมูล ณ เวลา ๐๙.๓๐ น. วันที่ ๒๗ พฤษภาคม พ.ศ. ๒๕๖๓ จากเว็บไซต์ Johns Hopkins University

[๒] เข้าถึงประกาศฉบับเต็มได้ที่ https://www.privacy.gov.ph/2020/05/npc-phe-bulletin-no-12-protecting-personal-data-in-a-work-from-home-arrangement/

มิใช่ขององค์กร การปฏิบัติงานจะต้องอยู่ภายใต้นโยบาย Bring Your Own Devices (BYOD)[๓] ขององค์กร

๒. อุปกรณ์พกพา หรืออุปกรณ์ที่สามารถเคลื่อนย้ายได้ (Removable Devices)

ผู้ปฏิบัติงานควรใช้อุปกรณ์พกพาหรืออุปกรณ์ที่สามารถเคลื่อนย้ายได้ อาทิ เมาส์ คีย์บอร์ด ประเภท USB แฟลชไดรฟ์ หรือ ดิสก์ ที่เป็นขององค์กรเท่านั้น กรณีที่ต้องจัดเก็บ หรือถ่ายโอนข้อมูลจำเป็นต้องตรวจสอบการเข้ารหัสจัดเก็บข้อมูล (Data Encryption) ที่ถูกต้องเพื่อรักษาความปลอดภัยของข้อมูลองค์กร

๓. ซอฟต์แวร์ (Software) หรือ ชุดคำสั่งที่ใช้สั่งงานระบบคอมพิวเตอร์

การปฏิบัติงานที่บ้านจำเป็นต้องใช้ซอฟต์แวร์ที่ได้รับอนุญาตหรือถูกออกแบบเพื่อวัตถุประสงค์การดำเนินงานขององค์กรเท่านั้น หลีกเลี่ยงการจัดเก็บเอกสารดิจิทัลของหน่วยงานหรือเอกสารที่มีข้อมูลส่วนบุคคลไว้ในซอฟต์แวร์ที่ไม่น่าเชื่อถือ

๔. การปรับปรุงข้อมูลระบบคอมพิวเตอร์และข้อมูลความปลอดภัยของคอมพิวเตอร์ให้เหมาะสมและเป็นปัจจุบัน (Proper configuration and security updates)

ทั้งก่อนและขณะที่ปฏิบัติงานที่บ้าน ผู้ปฏิบัติงานควรติดตั้งและปรับปรุงสถานะของ Security Patch หรือโปรแกรมซ่อมแซมจุดบกพร่องที่อาจส่งผลต่อความปลอดภัยของระบบคอมพิวเตอร์ ให้เป็นปัจจุบัน เพื่อป้องกันการโจมตี รักษาความปลอดภัยทางไซเบอร์ โดยสามารถทำได้โดยการปรับปรุงสถานะของระบบปฏิบัติการทางคอมพิวเตอร์ อาทิ การอัพเดท Windows และการดำเนินการดังต่อไปนี้

๔.๑ ติดตั้งระบบ security patches และตั้งค่าให้เป็นการอัพเดทโดยระบบอัตโนมัติ (Automatic update)

๔.๒ อัพเดทระบบป้องกันไวรัส (antivirus software) อย่างสม่ำเสมอ

๔.๓ ติดตั้งและตั้งค่าการอัพเดทระบบควบคุมการทำงานของคอมพิวเตอร์ (configuration) และ web browser ให้เป็นระบบอัตโนมัติ รวมถึงส่วนที่ใช้ปรับแต่งการใช้งานและการแสดงผลในส่วนต่าง ๆ ของคอมพิวเตอร์ (System Preferences)

๔.๔ ติดตั้งและอัพเดท Personal Productivity Software หรือระบบที่ช่วยเพิ่มประสิทธิภาพในการทำงาน อาทิ word processor โปรแกรมประมวลผลคำและการจัดการด้านเอกสาร หรือฟังก์ชันด้านการคำนวณโดยโปรแกรมการคำนวณแบบ spreadsheet

๔.๕ ติดตั้งและอัพเดทระบบการประชุมโดยการสื่อสารทางไกล

---

[๓] Bring Your Own Device คือกรณีที่พนักงานขององค์กรนำอุปกรณ์ส่วนบุคคล (Personal Device) เขามาใชงานภายในระบบเครือข่ายขององคกร ซึ่งปจจุบันไม่จำกัดเฉพาะเครื่องคอมพิวเตอร์ Notebook หรือ Netbook แต่รวมถึงอุปกรณ์ Smart Phone และ Tablet ทำใหระบบเครือข่ายมีเครื่องลูกข่ายเพิ่มมากขึ้น ซึ่งยากตอการดูแลรักษาความปลอดภัยของระบบ เนื่องจากนโยบายรักษาความปลอดภัยสำหรับการปฏิบัติการของเครื่องคอมพิวเตอร์ทั่วไปนั้น แตกตางจากนโยบายรักษาความปลอดภัยสำหรับอุปกรณ Smart Phone และ Tablet องค์กรจึงจำเป็นต้องกำหนดนโยบายรักษาความปลอดภัยในเรื่องนี้ใหชัดเจน มิฉะนั้นอาจเกิดปญหาตอการใชงานของผู้ใช้งานโดยรวมและความปลอดภัยของระบบเครือข่ายขององคกร โดยองค์กรสามารถเลือกใช้นโยบายรักษาความปลอดภัยได้ตามต้องการ ไม่ว่าจะเป็นการลงทะเบียนผู้ใช้งาน การยืนยันตัวตน การกำหนดสิทธิ์การเข้าถึงเครือข่าย การจัดเก็บบันทึก การตรวจสอบและยับยั้งการโจมตีเครือข่ายจากอุปกรณ์เหล่านั้น เป็นต้น

๕. การกำหนดค่า Web Browser

ผู้ปฏิบัติงานจำเป็นต้องตรวจสอบและอัพเดท Web Browser ให้เป็นปัจจุบัน และกำหนดค่าการปฏิบัติงานของ Web Browser ให้เหมาะสม อาทิ การตั้งค่า Internet Options ของ Chrome หรือ Firefox ให้ดำเนินการเพื่อรักษาความปลอดภัยของข้อมูลดังนี้

- ปิดการบันทึกรหัสผ่านโดยระบบอัตโนมัติ รวมถึงการชำระเงิน การแจ้งที่อยู่ หรือการระบุตัวตนในช่องทางการอื่น ๆ
- ใช้รหัสผ่านที่คาดเดายาก
- เปิดใช้งานระบบป้องกันการติดตาม หรือ DO NOT TRACK ในส่วนของ Internet Options เพื่อป้องกัน Web Browser ที่ติดตามการใช้งานเว็บไซต์ ซึ่งถือเป็นกลไกป้องกันความเป็นส่วนตัวของบุคคลจากการติดตามของแต่ละเว็บไซต์ที่เข้าเยี่ยมชม โดยเว็บไซต์จะทำการตรวจสอบพฤติกรรมการใช้งานเว็บไซต์ของผู้ใช้งาน รวมถึงการแชร์ข้อมูลต่าง ๆ ซึ่งอาจนำไปสู่การนำเสนอการบริการ หรือโฆษณาที่เจาะจงกลุ่มเป้าหมาย
- เปิดระบบแจ้งเตือนกรณีมีการพยายามเข้าถึงรหัสผ่าน
- ตั้งค่าการเข้าถึงการใช้งานเป็นระบบ “Ask first” หรือการตรวจสอบเพื่อยืนยันตัวตนก่อนการใช้งาน
- ลบข้อมูลส่วนบุคคลเมื่อออกจาก Web Browser

๖. การประชุมทางวิดีโอ

องค์กรควรใช้แพลตฟอร์มการประชุมออนไลน์ที่ได้ทำสัญญากับองค์กร และเป็นแพลตฟอร์มที่ได้มาตรฐานเรื่องความปลอดภัยและความเป็นส่วนตัว (privacy and security) กรณีมีความจำเป็นต้องใช้แพลตฟอร์มการประชุมที่ไม่เสียเงินหรือไม่ได้ทำสัญญากับองค์กร ให้ใช้รุ่นที่มีการอัพเดทและมีฟังก์ชันเรื่องความเป็นส่วนตัวและความปลอดภัย และตั้งค่าการใช้งานด้วยวิธีต่าง ๆ ดังนี้

๖.๑ ตั้งค่าการประชุมเป็นรูปแบบส่วนตัว (private)

๖.๒ ไม่เปิดเผยรหัสการเข้าประชุมในระบบที่เป็นสาธารณะ (public domains)

๖.๓ สร้างรหัสผ่านการเข้าถึงห้องประชุมสำหรับผู้เข้าร่วมประชุม

๖.๔ เมื่อจัดการประชุม ผู้จัดการประชุม (meeting host) ต้องตรวจสอบให้แน่ใจว่าได้รับการยืนยันตัวตนจากผู้เข้าร่วมประชุมแต่ละราย

๖.๕ ควบคุมหน้าจอแสดงผลและจัดทำการบันทึกอย่างระมัดระวัง

๖.๖ ปิดกล้องและไมโครโฟนเมื่อไม่มีคำกล่าว หรือไม่ได้ใช้งาน

๖.๙ หลีกเลี่ยงการถ่ายโอนไฟล์

<u>ความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับผู้ใช้งาน (Acceptable Use)</u>

องค์กรจะต้องจัดให้มีนโยบายความปลอดภัยระบบสารสนเทศสำหรับผู้ใช้งาน (Acceptable Use Policy - AUP) ที่จะกำหนดเกี่ยวกับการใช้งานอุปกรณ์ IT ส่วนบุคคล ซึ่งรวมถึงการใช้อีเมลส่วนตัว การเข้าถึงข่าวสาร โซเชียลมีเดีย การสตรีมมิ่งวิดีโอ และเครือข่ายต่าง ๆ ที่สามารถกำหนดเป็นนโยบายเฉพาะขององค์กร ซึ่งการใช้อุปกรณ์ที่เป็นสินทรัพย์ขององค์กรมีความจำเป็นต้องใช้สำหรับการปฏิบัติงานที่เป็นไปตามวัตถุประสงค์ขององค์กร การกำหนดนโยบายความปลอดภัยระบบสารสนเทศสำหรับผู้ใช้งานขององค์กร

ควรพิจารณากำหนดรูปแบบการใช้งานที่ไม่ได้รับอนุญาตหรือการใช้งานที่ไม่เป็นที่ยอมรับ ซึ่งอาจเป็นการกำหนดตามแนวทางดังต่อไปนี้

- ห้ามการใช้งานที่ขัดต่อกฎหมาย ประเพณี จริยธรรม และพฤติกรรมอันดี
- ห้ามการใช้งานเพื่อผลประโยชน์ส่วนบุคคล เช่น เพื่อความบันเทิง กิจกรรมที่มีวัตถุประสงค์เพื่อกำไร (profit-oriented) สร้างความเกลียดชัง (hostile) หรือการแบ่งแยก (partisan)
- ห้ามการใช้งานที่มีวัตถุประสงค์เพื่อทำลายความสมบูรณ์ ความน่าเชื่อถือ การรักษาความลับ และความมีประสิทธิภาพของระบบเทคโนโลยีสารสนเทศ
- ห้ามการใช้งานที่ละเมิดสิทธิของผู้ใช้งานรายอื่น

<u>การควบคุมการเข้าถึง (Access Control)</u>

การเข้าถึงข้อมูลขององค์กรจะต้องอยู่ภายใต้หลักความจำเป็นในการรู้ข้อมูล (need-to-know basis) ซึ่งจะเป็นการกำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานแต่ละราย โดยสิทธิดังกล่าวจะถูกกำหนดไว้ล่วงหน้าและถูกควบคุมด้วยระบบควบคุมอย่างรัดกุม

<u>การตรวจสอบผู้ใช้งาน</u>

การเข้าถึงบัญชีการใช้งานของบุคคลากรในองค์กร ผู้ปฏิบัติงานจำเป็นต้องกำหนดรหัสผ่านที่คาดเดาได้ยาก ซึ่งจะต้องมีความยาวอย่างน้อยแปดตัวอักษรประกอบด้วยตัวอักษรตัวใหญ่ ตัวอักษรตัวเล็ก ตัวเลขและสัญลักษณ์ และห้ามใช้รหัสผ่านร่วมกัน รวมถึงให้ตั้งค่า Multi-Factor Authentication[๔] หรือ กระบวนการรับรองความถูกต้องสำหรับทุกบัญชีเพื่อป้องกันผู้สวมสิทธิ และเพื่อให้สามารถตรวจสอบควบคุมบัญชีได้โดยทันที

<u>ความปลอดภัยของเครือข่าย (Network Security)</u>

เมื่อจำเป็นต้องเชื่อมต่ออุปกรณ์คอมพิวเตอร์ขององค์กรเข้ากับ Personal Hotspots หรือ Wi-Fi ของที่บ้าน จำเป็นต้องตระหนักถึงการดำเนินการดังต่อไปนี้

- ไม่ควรเข้าถึงหน้าเว็บ (webpage) ที่เป็นอันตราย ซึ่งพึงระวังโดยการค้นหาคำนำหน้า “https” บน URL ทุกครั้งเพื่อให้แน่ใจว่ามีการเข้ารหัสของเว็ตไซต์ที่เชื่อถือได้ (Encryption) รวมถึงตรวจสอบใบรับรองของเว็บไซต์เพื่อตรวจสอบข้อมูลผู้สร้างเว็บไซต์ที่เข้าใช้งาน

---

[๔] Muti-Factor Authentication (MFA) คือ กระบวนการรับรองความถูกต้องในการตรวจสอบและยืนยันตัวบุคคลเพื่อเพิ่มความปลอดภัยที่สูงขึ้นในการอนุญาตเข้าใช้งานซอฟต์แวร์ ระบบ หรือเข้าถึงข้อมูลต่าง ๆ ซึ่งโดยทั่วไประบบ MFA จะเป็นการใช้เครื่องมือตั้งแต่ ๒ ชนิดขึ้นไปในการตรวจสอบและยืนยันความถูกต้อง ดังนี้

- What you know เช่น password รหัสประจำตัว หรือ คำถามเฉพาะเพื่อกู้รหัสผ่าน
- What you have เช่น บัตรสมาร์ทการ์ด Fast IDentity Online token, one-time password (OTP), อุปกรณ์บลูทูธ, apple watch หรือ authenticator device อื่น ๆ
- Who you are เช่น ลายนิ้วมือ หรือ ระบบจดจำใบหน้า
- What you do and where you are เช่น การระบุที่อยู่ โดยใช้ GPS, IP Address หรือ Integrated Windows Authentication (IWA) และ พฤติกรรมการพิมพ์ (keystroke biometrics)

สืบค้นจาก https://www.vulcan-tec.com/MFA-vs-SSO.html เมื่อวันที่ ๑ พฤษภาคม พ.ศ. ๒๕๖๓

- การกำหนดค่า WiFi หรือ Router ต้องตรวจสอบให้เป็นการเชื่อมต่อกับอุปกรณ์ปัจจุบัน การเข้ารหัสและความปลอดภัยของการใช้ WiFi ควรกำหนดให้เป็นการเข้ารหัสขั้นสูง (Advanced Encryption Standard) และกำหนดรหัสผ่านที่คาดเดายาก
- หลีกเลี่ยงการเชื่อมต่อคอมพิวเตอร์ขององค์กรกับเครือข่ายสาธารณะ อาทิ Wi-Fi ของร้านกาแฟ หากมีความจำเป็นต้องใช้ให้ใช้เครือข่ายเสมือนส่วนตัว หรือ Virtual Private Network (VPN)[๕] ที่เชื่อถือได้ในการเชื่อมต่อ

<u>การบันทึกข้อมูลและความปลอดภัยของเอกสาร (Records and File Security)</u>

ควรกำหนดให้ผู้ปฏิบัติงานตั้งค่านโยบายเกี่ยวกับการประมวลผลข้อมูล การป้องกันและรักษาความลับของเอกสารบนอุปกรณ์ที่ใช้ปฏิบัติงาน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ซึ่งรวมถึงการตั้งค่าเกี่ยวกับนโยบายเรื่องต่าง ๆ ดังนี้

- นโยบายการจัดการการบันทึกข้อมูล (records management policy)
- นโยบายการป้องกันการเผยแพร่เอกสารสำคัญในช่องทางที่ไม่ได้รับอนุญาต เช่น บนเว็บไซต์ (policy against posting sensitive documents in unauthorized channels)
- นโยบายการจดจำขั้นตอนการประมวลผลข้อมูลที่สำคัญบนอุปกรณ์ส่วนบุคคล (retention policy for processing sensitive data in personal devices)

<u>การใช้งานอีเมล</u>

เมื่อผู้ปฏิบัติงานจำเป็นต้องใช้อีเมลในการถ่ายโอนข้อมูลสำคัญ ควรจัดทำการเข้ารหัสเอกสารและเอกสารแนบ[๖] รวมถึงตรวจสอบการใช้ช่องการส่งถึง สำเนาถึง และสำเนาลับถึง (TO, CC and BCC) อยู่เสมอ เพื่อหลีกเลี่ยงการส่งเอกสารไปยังผู้รับที่ไม่ถูกต้องหรือการเปิดเผยที่อยู่อีเมลของผู้อื่นแก่ผู้รับโดยไม่จำเป็น

<u>ความปลอดภัยทางกายภาพ (Physical security)</u>

เมื่อผู้ปฏิบัติงานปฏิบัติงานที่บ้านควรสร้างพื้นที่การทำงานให้มีความเป็นส่วนตัว ไม่ควรจัดวางคอมพิวเตอร์ในจุดที่ไม่เป็นเป้าสายตาให้ผู้อื่นสามารถเห็นถึงข้อมูลบนจอแสดงผลคอมพิวเตอร์ได้ และอาจปฏิบัติด้วยวิธีดังต่อไปนี้

- ตั้งค่าระบบล็อคอุปกรณ์ที่ใช้ในการทำงาน จัดเก็บเอกสารในพื้นที่ปลอดภัยเมื่อไม่ใช้งาน หากจำเป็นต้องพิมพ์เอกสารควรตรวจสอบให้แน่ใจว่าเอกสารทั้งรูปแบบดิจิทัลและเอกสารทางกายภาพได้ผ่านการดำเนินการตามนโยบายขององค์กรที่เหมาะสมแล้ว
- ไม่ควรวางเอกสารที่มีข้อมูลสำคัญทิ้งไว้โดยรอบจุดปฏิบัติงาน และไม่นำมาใช้เป็นกระดาษจดบันทึก (scratch paper)

---

[๕] VPN หรือ Virtual Private Network หมายถึง เครือข่ายเสมือนส่วนตัว ที่ทำงานโดยใช้โครงสร้างของเครือข่ายสาธารณะ หรือบนเครือข่ายไอพี แต่ยังสามารถคงความเป็นเครือข่ายเฉพาะขององค์กรได้ด้วยการเข้ารหัสก่อนส่ง เพื่อให้ข้อมูลมีความปลอดภัยมากขึ้น สืบค้นจาก https://vpn.ku.ac.th/index.php?content=whatisvpn เมื่อวันที่ ๓ พฤษภาคม พ.ศ. ๒๕๖๓

[๖] ตัวอย่างการเข้ารหัสเอกสารสำหรับ Microsoft Word สามารถทำได้โดยฟังก์ชัน Protect Document ซึ่งจะเป็นการกำหนดให้มีรหัสผ่านสำหรับการเปิดใช้งานเอกสารนั้น ๆ

การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident Management)

ผู้ปฏิบัติงานจะต้องแจ้งหัวหน้างานทันทีในกรณีที่มีหรืออาจมีการละเมิดข้อมูลส่วนบุคคลในช่วงที่ปฏิบัติงานจากที่บ้าน และควรแจ้งต่อเจ้าหน้าที่คุ้มครองข้อมูลขององค์กร และ/หรือ ทีมงานผู้ทำหน้าที่ดูแลข้อมูลขององค์กรโดยทันที

****