LAW for ASEAN
by the Office of the Council of State of Thailand

แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลจากการปฏิบัติงานที่บ้าน ของประเทศฟิลิปปินส์

(Protecting Personal Data in a Work From Home Arrangement)

คณะกรรมการข้อมูลส่วนบุคคลของประเทศฟิลิปปินส์ (National Privacy Commission – NPC) ได้ออกประกาศชื่อ "NPC PHE Bulletin No.12: Protecting Personal Data in a Work From Home Arrangement" เพื่อให้คำแนะนำแก่องค์กรที่มีการจัดให้บุคลากรปฏิบัติงานที่บ้านและเป็นแนวทางในการคุ้มครองข้อมูลส่วนบุคคล โดยมีสาระสำคัญ ดังนี้

ความปลอดภัยของเครือข่าย (Network Security)

เมื่อจำเป็นต้องเชื่อมต่ออุปกรณ์คอมพิวเตอร์ขององค์กรเข้ากับ Personal Hotspots หรือ Wi-Fi ของที่บ้าน

- ไม่ควรเข้าถึงหน้าเว็บ (webpage) ที่เป็นอันตราย พึงระวังโดยการค้นหาคำนำหน้า "https" บน URL ทุกครั้ง เพื่อให้แน่ใจว่ามีการเข้ารหัสของเว็บไซต์ที่เชื่อถือได้ (Encryption)
- ตรวจสอบ WiFi หรือ Router ให้เป็นการเชื่อมต่อกับอุปกรณ์ปัจจุบัน
- การเข้ารหัสและความปลอดภัยของการใช้ WiFi ควรกำหนดให้เป็นการเข้ารหัสขั้นสูง (Advanced Encryption Standard) และกำหนดรหัสผ่านที่คาดเดายาก
- หลีกเลี่ยงการเชื่อมต่อคอมพิวเตอร์ขององค์กรกับเครือข่ายสาธารณะ อาทิ Wi-Fi ของร้านกาแฟ หากมีความจำเป็นต้องใช้ให้ใช้เครือข่ายเสมือนส่วนตัว หรือ Virtual Private Network (VPN) ที่เชื่อถือได้ในการเชื่อมต่อ

ด้านระบบและอุปกรณ์คอมพิวเตอร์

- องค์กรควรจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่เหมาะสมเพียงพอต่อการปฏิบัติงานของบุคลากร (Computers and other ICT peripherals) กรณีที่ไม่สามารถจัดหาอุปกรณ์ได้เพียงพอและจำเป็นต้องให้ใช้อุปกรณ์ส่วนบุคคลที่มีใช้ขององค์กร การปฏิบัติงานจะต้องอยู่ภายใต้นโยบาย Bring Your Own Devices (BYOD) ขององค์กร
- ผู้ปฏิบัติงานควรใช้อุปกรณ์พกพาหรืออุปกรณ์ที่สามารถเคลื่อนย้ายได้ อาทิ เมาส์ คีย์บอร์ด ประเภท USB แฟลชไดรฟ์ หรือ ดิสก์ ที่เป็นขององค์กรเท่านั้น กรณีที่ต้องจัดเก็บหรือถ่ายโอนข้อมูล จำเป็นต้องจัดทำและตรวจสอบการเข้ารหัสจัดเก็บข้อมูล (Data Encryption) ที่ถูกต้องเพื่อรักษาความปลอดภัยของข้อมูลขององค์กร
- จำเป็นต้องใช้ซอฟต์แวร์ที่ได้รับอนุญาตหรือถูกออกแบบเพื่อวัตถุประสงค์การดำเนินงานขององค์กรเท่านั้น และหลีกเลี่ยงการจัดเก็บเอกสารดิจิทัลขององค์กร หรือเอกสารที่มีข้อมูลส่วนบุคคลไว้ในซอฟต์แวร์ที่ไม่น่าเชื่อถือ
- ก่อนและขณะที่ปฏิบัติงานที่บ้าน ผู้ปฏิบัติงานควรติดตั้งและปรับปรุงสถานะของระบบ Security Patch หรือโปรแกรมซ่อมแซมจุดบกพร่องที่อาจส่งผลต่อความปลอดภัยของระบบคอมพิวเตอร์ ให้เป็นปัจจุบัน เพื่อป้องกันการโจมตี โดยสามารถทำได้โดยการปรับปรุงสถานะของระบบปฏิบัติการทางคอมพิวเตอร์ อาทิ การอัพเดท Windows และตั้งค่าให้เป็นการอัพเดทโดยระบบอัตโนมัติ รวมถึงการปรับปรุงระบบป้องกันไวรัส (antivirus software) อย่างสม่ำเสมอ
- ติดตั้งและอัพเดทระบบการประชุมโดยการสื่อสารทางไกล

การประชุมทางวิดีโอ

ควรใช้แพลตฟอร์มการประชุมออนไลน์ที่ได้ทำสัญญากับองค์กร และเป็นแพลตฟอร์มที่ได้มาตรฐานเรื่องความปลอดภัยและความเป็นส่วนตัว (privacy and security) กรณีมีความจำเป็นต้องใช้แพลตฟอร์มการประชุมที่ไม่เสียเงินหรือไม่ได้ทำสัญญากับองค์กร ให้ใช้รุ่นที่มีการอัพเดทและมีฟังก์ชันเรื่องความเป็นส่วนตัวและความปลอดภัย ตั้งค่าและใช้งานด้วยวิธีต่าง ๆ ดังนี้

- ตั้งค่าการประชุมเป็นรูปแบบส่วนตัว (private)
- ไม่เปิดเผยรหัสการเข้าประชุมในระบบที่เป็นสาธารณะ (public domains)
- สร้างรหัสผ่านการเข้าถึงห้องประชุมสำหรับผู้เข้าร่วมประชุม
- เมื่อจัดการประชุม ผู้จัดการประชุม (meeting host) ควรตรวจสอบให้แน่ใจว่าได้รับการยืนยันตัวตนจากผู้เข้าร่วมประชุมแต่ละราย
- ควบคุมหน้าจอแสดงผลและจัดทำการบันทึกอย่างระมัดระวัง
- ปิดกล้องและไมโครโฟนเมื่อไม่มีคำกล่าว หรือไม่ได้ใช้งาน

การตรวจสอบผู้ใช้งาน

การเข้าถึงบัญชีการใช้งานของบุคลากรในองค์กร ผู้ปฏิบัติงานจำเป็นต้องกำหนดรหัสผ่านที่คาดเดาได้ยาก ซึ่งจะต้องมีความยาวอย่างน้อยแปดตัวอักษรประกอบด้วยตัวอักษรตัวใหญ่ ตัวอักษรตัวเล็ก ตัวเลข และสัญลักษณ์ และห้ามใช้รหัสผ่านร่วมกัน รวมถึงให้จัดทำ Multi-Factor Authentication หรือ กระบวนการรับรองความถูกต้องที่สูงขึ้นสำหรับทุกบัญชี อาทิ การใช้ one-time password (OTP) ลายนิ้วมือ ระบบจดจำใบหน้า หรือ Fast IDentity Online token เพื่อป้องกันผู้สวมสิทธิและเพื่อให้สามารถตรวจสอบควบคุมบัญชีได้โดยทันที

การควบคุมการเข้าถึง (Access Control)

การเข้าถึงข้อมูลของบุคลากรจะต้องอยู่ภายใต้หลัก Need to Know Basis หรือหลักความจำเป็นในการรับรู้ข้อมูล ซึ่งจะเป็นการกำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานแต่ละราย โดยสิทธิดังกล่าวจะถูกกำหนดไว้ล่วงหน้า และถูกควบคุมด้วยระบบควบคุมอย่างรัดกุม

การใช้งาน Web Browser

ตั้งค่า Internet Options ให้เป็นปัจจุบัน อาทิ การใช้งาน Chrome หรือ Firefox ควรดำเนินการเพื่อรักษาความปลอดภัยของข้อมูลดังนี้

- ปิดการบันทึกรหัสผ่านโดยระบบอัตโนมัติ รวมถึงระบบการชำระเงิน การแจ้งที่อยู่ หรือการระบุตัวตนในช่องทางการอื่น ๆ
- ใช้รหัสผ่านที่คาดเดายาก และเปิดระบบแจ้งเตือนกรณีมีการพยายามเข้าถึงรหัสผ่าน
- ตั้งค่าการเข้าถึงการใช้งานเป็นระบบ "Ask first" หรือการตรวจสอบเพื่อยืนยันตัวตนก่อนการใช้งาน
- เปิดใช้งานระบบป้องกันการติดตาม หรือ DO NOT TRACK ในช่อง Internet Options เพื่อป้องกัน Web Browser ที่ติดตามการเข้าใช้งานเว็บไซต์ ซึ่งกลไกดังกล่าวถือเป็นการคุ้มครองความเป็นส่วนตัวของบุคคลจากการติดตามของเว็บไซต์ที่เข้าเยี่ยมชม โดยเว็บไซต์จะทำการตรวจสอบพฤติกรรมการใช้งานเว็บไซต์ของผู้ใช้งาน รวมถึงการแชร์ข้อมูลต่าง ๆ ซึ่งอาจนำไปสู่การนำเสนอการบริการ หรือโฆษณาที่เจาะจงกลุ่มเป้าหมาย
- ลบข้อมูลส่วนบุคคลเมื่อออกจาก Web Browser

การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident Management)

ผู้ปฏิบัติงานจะต้องแจ้งหัวหน้างานทันทีในกรณีที่มีหรืออาจมีการละเมิดข้อมูลส่วนบุคคลในช่วงที่ปฏิบัติงานที่บ้าน และควรแจ้งต่อเจ้าหน้าที่คุ้มครองข้อมูลขององค์กร และ/หรือ ทีมงานผู้ทำหน้าที่ดูแลข้อมูลขององค์กรโดยทันที

การใช้งานอีเมล

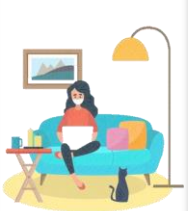
เมื่อจำเป็นต้องใช้อีเมลในการถ่ายโอนข้อมูลสำคัญ ควรจัดทำการเข้ารหัสเอกสารและเอกสารแนบ รวมถึงตรวจสอบการใช้ช่องการส่งถึง สำเนาถึง และสำเนาลับถึง (TO, CC and BCC) อยู่เสมอ เพื่อหลีกเลี่ยงการส่งเอกสารไปยังผู้รับที่ไม่ถูกต้องหรือการเปิดเผยที่อยู่อีเมลของผู้อื่นแก่ผู้รับโดยไม่จำเป็น

ความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับผู้ใช้งาน (Acceptable Use)

องค์กรจะต้องจัดให้มี Acceptable Use Policy หรือนโยบายความปลอดภัยระบบสารสนเทศสำหรับผู้ใช้งานที่จะกำหนดเกี่ยวกับการใช้งานอุปกรณ์ IT ส่วนบุคคล ซึ่งรวมถึงการใช้อีเมลส่วนตัว การเข้าถึงข่าวสาร โซเชียลมีเดีย การสตรีมมิ่งวิดีโอ และเครือข่ายต่าง ๆ ที่สามารถกำหนดเป็นนโยบายเฉพาะขององค์กร ซึ่งการใช้อุปกรณ์ที่เป็นสินทรัพย์ขององค์กรจำเป็นต้องใช้สำหรับการปฏิบัติงานที่เป็นไปตามวัตถุประสงค์ขององค์กรเท่านั้น

การกำหนดนโยบายความปลอดภัยระบบสารสนเทศสำหรับผู้ใช้งานขององค์กรควรพิจารณากำหนดรูปแบบการใช้งานที่ไม่ได้รับอนุญาตหรือการใช้งานที่ไม่เป็นที่ยอมรับ ซึ่งอาจกำหนดได้ตามแนวทางดังต่อไปนี้

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



ความปลอดภัยทางกายภาพ (Physical security)

เมื่อปฏิบัติงานที่บ้านควรสร้างพื้นที่การทำงานให้มีความเป็นส่วนตัว ไม่ควรจัดวางคอมพิวเตอร์ในจุดที่เป็นเป้าสายตาให้ผู้อื่นสามารถเห็นถึงข้อมูลบนจอแสดงผลคอมพิวเตอร์ได้ และอาจปฏิบัติด้วยวิธีดังต่อไปนี้

- ตั้งค่าระบบล็อคอุปกรณ์ที่ใช้ในการทำงาน จัดเก็บเอกสารในพื้นที่ปลอดภัยเมื่อไม่ใช้งาน หากจำเป็นต้องพิมพ์เอกสารควรตรวจสอบให้แน่ใจว่าเอกสารทั้งรูปแบบดิจิทัลและเอกสารทางกายภาพได้ผ่านการดำเนินการตามนโยบายขององค์กรที่เหมาะสมแล้ว
- ไม่ควรวางเอกสารที่มีข้อมูลสำคัญทิ้งไว้โดยรอบจุดปฏิบัติงาน และไม่นำมาใช้เป็นกระดาษจดบันทึก (scratch paper)

เข้าถึงบทความฉบับเต็มได้ที่นี่ >>>

ฝ่ายอาเซียนและกิจการต่างประเทศ กองกฎหมายต่างประเทศ
สำนักงานคณะกรรมการกฤษฎีกา