ประกาศคณะศึกษาศาสตร์ มหาวิทยาลัยมหาสารคาม
เรื่อง การป้องกันความปลอดภัยทางไซเบอร์

ตามนโยบายความมั่นคงปลอดภัยทางไซเบอร์ของมหาวิทยาลัยมหาสารคาม พ.ศ. ๒๕๖๖-๒๕๖๙ ได้ทำการเผยแพร่นโยบายและแนวปฏิบัติฯ ให้แก่คณะ/หน่วยงานได้รับทราบ เพื่อนำไปปรับใช้ให้เกิดความมั่นคงปลอดภัยทางไซเบอร์ นั้น ในการนี้ คณะศึกษาศาสตร์ มหาวิทยาลัยมหาสารคาม จึงขอประกาศแนวปฏิบัติในการป้องกันความปลอดภัยทางไซเบอร์ ให้ผู้บริหาร ข้าราชการ พนักงาน เจ้าหน้าที่ และบุคลากรทุกคนในสังกัดคณะศึกษาศาสตร์ มหาวิทยาลัยมหาสารคาม ได้รับทราบและสื่อสารเพื่อความเข้าใจและปฏิบัติตามแนวนโยบายมาตรฐานดังนี้

ข้อ ๑ ไม่ตั้งรหัสผ่านที่ง่ายเกินไปและเปลี่ยนรหัสบ่อย ๆ

รหัสผ่านเป็นกุญแจที่ไขเข้าสู่ข้อมูล และเอกสารของเรา อาชญากรไซเบอร์จะใช้วิธีการต่าง ๆ เพื่อที่จะเข้าผ่าน เข้ารหัสให้ได้ เพื่อที่จะไม่ให้คนเหล่านั้นเข้าถึงได้ง่าย ควรตั้งรหัสที่ยาก ซับซ้อน และไม่ควรบันทึกรหัสผ่านไว้ในอุปกรณ์ดิจิทัล

ข้อ ๒ สำรองข้อมูล (Backup) ไว้เสมอ

การสำรองข้อมูลเป็นเรื่องสำคัญที่จะปกป้องข้อมูลที่สำคัญ เพื่อป้องกันการทำข้อมูลสูญหาย ทั้งที่ตั้งใจและไม่ตั้งใจ เพราะการแก้ไขข้อมูลปัจจุบันมีปัญหา หรือไฟล์ที่ใช้งานไม่ได้ และต้องการกลับไปใช้ข้อมูลเก่าก่อนหน้านี้ การป้องกันการติดไวรัส และโจรกรรมข้อมูลจากทาง Hacker

ข้อ ๓ ระมัดระวังการหลอกลวงให้กรอกข้อมูล (Phishing)

มิจฉาชีพจะปลอมตัวเป็นองค์กรที่เป็นที่รู้จัก และหลอกล่อให้ผู้ใช้งานเปิดเผยข้อมูลส่วนตัว เพื่อจะเข้ารหัสผ่านหรือเพื่อติดตั้งมัลแวร์ (Malware) ควรสังเกต URL ของเว็บไซต์ให้ชัดเจนและอย่ากดลิ้งก์หรือเปิดไฟล์ที่แนบเข้ามา ระมัดระวังการหลอกลวงของแก๊งค์คอลเซ็นเตอร์ที่พยายามล้วงข้อมูลส่วนตัว และนำไปเปิดบัญชีอินเทอร์เน็ตแบงกิ้งที่สามารถโอนเงินจากบัญชีธนาคารของผู้ใช้งานออกไปได้

ข้อ ๔ ใช้สื่อสังคมออนไลน์อย่างระมัดระวัง

ไม่ควรรับคนที่ไม่รู้จักเป็นเพื่อน หลีกเลี่ยงการแชตกับคนแปลกหน้า ไม่เปิดเผยข้อมูลส่วนตัวในโหมดสาธารณะ และลบบัญชีสื่อสังคมออนไลน์ที่ไม่ได้ใช้แล้ว

ข้อ ๕ ใส่ใจกับการตั้งค่าความเป็นส่วนตัว

แอปส่วนใหญ่จะมีตัวเลือกในการตั้งค่าความเป็นส่วนตัวให้แก่ผู้ใช้งาน เพื่อที่จะตัดสินใจได้ว่าข้อมูลไหน จะแบ่งปันให้ใครได้เท่าไร ทางที่ดีควรจะเลือกตั้งค่าให้มีความเป็นส่วนตัวให้มากที่สุด ระมัดระวังในการเปิดเผยชื่อและที่ตั้งของเรา และปฏิเสธแอปที่พยายามจะเข้าถึงกล้องถ่ายรูปของเรา

ข้อ ๖ ระมัดระวังการโพสต์ Digital Footprint ในสื่อสังคมออนไลน์

สิ่งที่ผู้ใช้โพสต์ลงโลกออนไลน์แล้ว สิ่งนั้นจะคงอยู่ตลอดไป แม้ว่าโพสต์ต้นทางจะลบแล้ว คนอื่นก็จะตามร่องรอยเราจนได้ เมื่อคิดจะโพสต์ ควรโพสต์แต่เรื่องที่ดี ๆ และระมัดระวังการเปิดเผยข้อมูลส่วนตัว

ข้อ ๗ ควรติดตั้งโปรแกรมรักษาความปลอดภัยให้กับอุปกรณ์ดิจิทัลทุกตัว
รวมถึงโทรศัพท์ด้วย เพื่อที่จะปกป้องอุปกรณ์เหล่านั้นจากภัยคุกคามในโลกไซเบอร์

ข้อ ๘ ติดตั้งเครื่องมือติดตามอุปกรณ์หรือล็อคหน้าจอ
ในกรณีที่ทำหาย เพื่อป้องกันไม่ให้ผู้อื่นนำไปเข้าถึงข้อมูลในเครื่องได้

ข้อ ๙ ระมัดระวังการใช้บลูทูธ (Bluetooth)
ถึงแม้ว่าจะสะดวกสบาย แต่บลูทูธก็ยังมีความเสี่ยงด้านความปลอดภัย ควรจะปิดโหมดบริการนี้ไว้เสมอเมื่อไม่ได้ใช้งาน

ข้อ ๑๐ อัปเดตระบบปฏิบัติการอยู่เสมอ
ทั้งระบบปฏิบัติการของอุปกรณ์ ดิจิทัล และโปรแกรมและแอปพลิเคชั่นที่ติดตั้งในอุปกรณ์นั้น เพื่อที่จะรับบริการด้านความปลอดภัย และซ่อมแซมข้อบกพร่องของรุ่นเก่า ๆ

ข้อ ๑๑ ระมัดระวังการใช้เครือข่ายไร้สาย (Wi-Fi)
อุปกรณ์เครือข่ายไร้สาย (Wi-Fi) ที่ใช้ควรจะมีความปลอดภัย ควรตั้งรหัสผ่านไว้ตลอดเวลา และไม่ใช้ Wi-Fi สาธารณะ เมื่อต้องเปิดเผย Wi-Fi ข้อมูลส่วนตัวหรือทำธุรกรรม

ข้อ ๑๒ ลบข้อมูลหรือโปรแกรมที่ไม่ได้ใช้งานแล้ว
หากว่ามีโปรแกรม หรือแอปที่ไม่ได้ใช้งานหลายเดือนแล้ว ควรลบ เช่นเดียวกับข้อมูลที่ไม่ได้ใช้แล้ว ควรจะลบออก หรือไม่ก็ควรจะเก็บข้อมูลเหล่านั้น ในฮาร์ดไดร์ฟต่างหาก หรือเก็บไว้ในลักษณะออฟไลน์ เพื่อที่จะปกป้องข้อมูลส่วนตัว ในกรณีที่ผู้ใช้งานอาจจะลืม

จึงประกาศมาให้ทราบโดยทั่วกัน และให้บุคลากรทุกคนถือปฏิบัติโดยเคร่งครัด

ประกาศ ณ วันที่ ๑ มีนาคม พ.ศ. ๒๕๖๖

(รองศาสตราจารย์ ดร.ชวลิต ชูกำแพง)
คณบดีคณะศึกษาศาสตร์ ปฏิบัติราชการแทน
ผู้รักษาราชการแทนอธิการบดีมหาวิทยาลัยมหาสารคาม