โรงเรียนจอมสุรางค์อุปถัมภ์
เลขรับ 0009
วันที่ - 3 ม.ค. 2566
เวลา.....

ด่วนที่สุด
ที่ ศธ ๐๔๓๑๘/ว๕

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษา
พระนครศรีอยุธยา
โรงเรียนอยุธยาวิทยาลัย ๕๓ หมู่ ๒
ถนนป่าโทน พระนครศรีอยุธยา ๑๓๐๐๐

๓ มกราคม ๒๕๖๕

เรื่อง การปฏิบัติหรือวิธีปฏิบัติเพื่อให้เกิดความปลอดภัยทางไซเบอร์

เรียน ผู้อำนวยการโรงเรียนในสังกัด

สิ่งที่ส่งมาด้วย คำแนะนำการปฏิบัติหรือวิธีปฏิบัติเพื่อให้เกิดความปลอดภัยทางไซเบอร์ จำนวน ๑ ฉบับ

ด้วย สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ได้รับแจ้งจากสำนักงานคณะกรรมการรักษาความความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เกี่ยวกับการโจมตีต่อเว็บไซต์ของหน่วยงานการศึกษา รวมถึงการประกาศขายข้อมูลของหน่วยงานการศึกษาทั้งในส่วนของสำนักงานเขตพื้นและสถานศึกษาในสังกัดสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

ในการนี้ สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพระนครศรีอยุธยา ขอให้ทุกโรงเรียนในสังกัดให้ความสำคัญต่อความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ การป้องกันเพื่อลดความเสี่ยงที่จะถูกโจมตี รวมถึงการดำเนินการเบื้องต้นสำหรับกรณีการรั่วไหลของข้อมูล เพื่อลดความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ โดยสามารถศึกษารายละเอียดคำแนะนำการปฏิบัติหรือวิธีปฏิบัติเพื่อให้เกิดความปลอดภัยทางไซเบอร์ได้ที่สิ่งที่ส่งมาพร้อมหนังสือฉบับนี้

จึงเรียนมาเพื่อทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นายบัญชา ปลื้มอารมย์)
รองผู้อำนวยการสำนักงานเขตพื้นที่การศึกษา ปฏิบัติราชการแทน
ผู้อำนวยการสำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพระนครศรีอยุธยา

เรียน ผู้อำนวยการ เพื่อ
☑ ๑. ทราบ
☐ ๒. สมควรมอบฝ่าย..... 4 ฝ่าย
พิจารณา/ดำเนินการ
☐ ๓. .....
- 3 ม.ค. 2566

-ทราบ
- แจ้งประชาสัมพันธ์คุณครูและนักเรียนทราบ
๓ ม.ค. ๒๕๖๖

☑ ทราบ ☐ อนุญาต ☐ อนุมัติ
☑ มอบ ☑ บริหารวิชาการ
☑ บริหารงานบุคคล
☑ บริหารงบประมาณฯ
☑ บริหารทั่วไป
☐ สำนักงานผู้อำนวยการ
๓ ม.ค.

กลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและการสื่อสาร
โทร. ๐ ๓๕๘๘ ๑๒๒๐
ไปรษณีย์อิเล็กทรอนิกส์ : spm@spmay.go.th

3 ม.ค. 66

คำแนะนำการปฏิบัติหรือวิธีปฏิบัติเพื่อให้เกิดความปลอดภัยทางไซเบอร์

๑. คำแนะนำในการปฏิบัติเพื่อลดความเสี่ยงที่จะถูกโจมตีเว็บไซต์โดยทั่วไป

ผู้ที่เป็นเจ้าของเว็บไซต์ควรจะต้องดำเนินการตรวจสอบว่าเว็บไซต์มีช่องโหว่ที่จุดใดและควรดำเนินการแก้ไขเพื่อไม่ให้ผู้ที่ไม่หวังดีใช้เป็นที่กระทำความผิดต่อไป โดยทั่วไปแล้วในเบื้องต้น ผู้ดูแลระบบควรจะเปลี่ยนรหัสผ่านของผู้ใช้ทั้งหมด ลบลิงก์ที่ไม่ได้ใช้งานออกจากเว็บไซต์ กำหนดสิทธิ์ในการเข้าถึงเว็บไซต์ใหม่ทั้งหมด จากนั้นจึงดำเนินการทดสอบหาช่องโหว่ของเว็บไซต์เพื่อป้องกันการโจมตีต่อไป

คำแนะนำสำหรับจัดทำเว็บไซต์โดยทั่วไปนั้นมีคำแนะนำจาก OWASP TOP 10 Project[๒] ซึ่งเป็นขององค์กรที่ชื่อ OWASP เป็นองค์กรที่ไม่แสวงหาผลกำไรที่ให้ความรู้ เพื่อการปรับปรุงในการจัดทำเว็บไซต์ให้ปลอดภัย ซึ่งมีคำแนะนำหลายเรื่อง เช่น การเขียนโปรแกรม การใช้เครื่องมือในการตรวจสอบการรักษาความมั่นคงปลอดภัย เทคโนโลยีที่ใช้ในการรักษาความมั่นคงปลอดภัยของเว็บไซต์ ซึ่งสามารถไปศึกษาและดาวน์โหลดเอกสารได้ที่ https://owasp.org/

๒. คำแนะนำในการดำเนินการเบื้องต้นสำหรับกรณีการรั่วไหลของข้อมูล

ตรวจสอบข้อมูลตามที่ปรากฏบนหน้าเว็บข้อมูลคอมพิวเตอร์ในระบบข้อมูล Log file และพฤติการณ์แวดล้อมในระบบ เพื่อประเมินว่ามีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่หากพบว่ามีเหตุการณ์เกิดขึ้นให้ดำเนินการเพื่อป้องกันรับมือและลดความเสี่ยงตาม พ.ร.บ. ไซเบอร์ฯ หรือแนวทางด้าน Cybersecurity เช่น NIST Cybersecurity Framework[๑] เป็นต้น ดำเนินการตรวจสอบข้อมูลที่มีความละเอียดอ่อนที่ถูกทำให้เผยแพร่ไป โดยได้อ้างว่าเป็นของหน่วยงานหรือบุคคลอื่น เพื่อพิจารณาแนวทางป้องกันและรับมือกับข้อกฎหมายและความเสียหายที่อาจจะเกิดขึ้น การดำเนินการเรื่องรับมือและตอบสนองเหตุการณ์ดังกล่าว นอกจากการกู้คืนระบบให้สามารถทำงานได้ตามปกติโดยเร็วแล้ว ควรจะดำเนินการหาสาเหตุและแหล่งที่มาของภัยคุกคามที่แท้จริงสามารถระบุร่องรอยได้ตามพยานหลักฐานที่ปรากฏได้อย่างชัดเจน ทั้งนี้ เพื่อเป็นการตรวจหาภัยคุกคามที่ยังคงแฝงอยู่ในระบบและเป็นการป้องกันไม่ให้เกิดเหตุซ้ำจากช่องโหว่ที่มีอยู่ในระบบ

อ้างอิง ๑. https://www.nist.gov/cyberframework
๒. https://owasp.org/www-project-top-ten/