



นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
(Information Security Policy)
โรงเรียนห้วยกรดวิทยา
พ.ศ. 2562

จัดทำโดย
กลุ่มงานระบบไอซีทีโรงเรียนห้วยกรดวิทยา
(กุมภาพันธ์ 2562)

คำนำ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2559 ในมาตรา 5 “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดย หน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทาง อิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ หน่วยงานของรัฐ พ.ศ. 2553 กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

กลุ่มงานระบบไอซีทีโรงเรียนห้วยกรดวิทยา ได้จัดทำนโยบาย เรื่อง แนวทางปฏิบัติในการควบคุมการ ปฏิบัติงานและรักษาความปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ โรงเรียนห้วยกรดวิทยา ตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงานภาครัฐตามมาตรา 7 ในพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงเรียนห้วยกรดวิทยา มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยี สารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ งานระบบไอซีทีจึงได้ทำนโยบายและแนว ปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โรงเรียนห้วยกรดวิทยา ปี 2562 โดย กำหนดให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบ เทคโนโลยีสารสนเทศ และสอดคล้องตามพระราชกฤษฎีกาฯ และประกาศฯ ดังกล่าวข้างต้น

กลุ่มงานระบบไอซีทีโรงเรียนห้วยกรดวิทยา
(กุมภาพันธ์ 2562)



บันทึกข้อความ

ส่วนราชการ โรงเรียนห้วยกรดวิทยา

ที่

วันที่ 18 กุมภาพันธ์ พ.ศ. 2562

เรื่อง ขออนุมัตินโยบายนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

(Information Security Policy) โรงเรียนห้วยกรดวิทยา พ.ศ. 2562

เรียน ผู้อำนวยการโรงเรียนห้วยกรดวิทยา

งานระบบไอซีทีโรงเรียนห้วยกรดวิทยา ได้จัดทำร่างนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policy) โรงเรียนห้วยกรดวิทยา พ.ศ. 2562 ซึ่งเป็นการปฏิบัติตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2559 ในมาตรา 5 “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดย หน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้”

เพื่อใช้เป็นแนวทางปฏิบัติให้กับผู้บริหาร เจ้าหน้าที่และบุคลากรภายนอกที่ปฏิบัติให้กับองค์กร รับทราบและตระหนักถึงความสำคัญ ตลอดจนความเหมาะสมในการใช้งานระบบเทคโนโลยีสารสนเทศ และการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของโรงเรียนห้วยกรดวิทยา และมอบหมายให้กลุ่มงานระบบไอซีที โรงเรียนห้วยกรดวิทยา เป็นผู้ดูแลระบบตามนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policy) โรงเรียนห้วยกรดวิทยา พ.ศ. 2562

จึงเรียนมาเพื่อโปรดพิจารณาอนุมัติ นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policy) โรงเรียนห้วยกรดวิทยา พ.ศ. 2562 เพื่อขับเคลื่อนสู่การปฏิบัติต่อไป

(นายสุเมธ ราชประชุม)

ตำแหน่งครูโรงเรียนห้วยกรดวิทยา

หัวหน้างานระบบไอซีทีโรงเรียนห้วยกรดวิทยา



ประกาศ

โรงเรียนห้วยกรดวิทยา

ว่าด้วยนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

(Information Security Policy)

การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นการจัดทำขึ้นเพื่อกำหนดแนวทางไว้ เพื่อยกระดับมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงเรียนห้วยกรดวิทยา ให้อยู่ระดับมาตรฐานสากล อีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการกู้คืนระบบอย่างรวดเร็ว และเป็นแนวทางปฏิบัติของผู้ใช้งานด้านเทคโนโลยีสารสนเทศของโรงเรียน นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงเรียนห้วยกรดวิทยา ประกอบด้วย 9 หมวด โดยมี รายละเอียดดังต่อไปนี้

หมวด 1

การพิสูจน์ตัวตน (Accountability, Identification and Authentication)

- ข้อ 1 ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)
- ข้อ 2 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีชื่อผู้ใช้งาน (Username) ไม่ว่าจะการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม
- ข้อ 3 ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษรไม่ น้อยกว่า 4 ตัวอักษร และยากต่อการคาดเดาได้
- ข้อ 4 ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๆ 6 เดือน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน
- ข้อ 5 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพยากรหรืออุปกรณ์ด้านเทคโนโลยีสารสนเทศของโรงเรียนห้วยกรดวิทยา และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านโดนล๊อค กีด หรือเกิดจากความผิดพลาดใดๆ กีด ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย
 - (1) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูล ซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้
 - (2) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ให้ออกจากระบบที่ทำงานอยู่ทุกครั้ง

หมวด 2

การบริหารจัดการทรัพย์สิน (Assets Management)

- ข้อ 6 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่โรงเรียนมอบไว้ให้ใช้งาน เสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง
- ข้อ 7 ผู้ใช้งานต้องไม่ให้อื่นยืมเครื่องคอมพิวเตอร์ หรือโน้ตบุ๊ก ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้น ได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ
- ข้อ 8 ทรัพย์สินและอุปกรณ์ด้านเทคโนโลยีสารสนเทศต่างๆ ที่โรงเรียนจัดเตรียมไว้ให้ใช้งาน มีวัตถุประสงค์เพื่อการใช้งานของโรงเรียนห้วยกรดวิทยาเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและอุปกรณ์ด้านเทคโนโลยีสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่โรงเรียนไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อโรงเรียน
- ข้อ 9 ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ 8 ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งาน ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น
- ข้อ 10 ผู้ใช้งานมีหน้าที่ต้องชดเชยค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่า ทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

หมวด 3

การบริหารจัดการข้อมูลองค์กร (Corporate Management)

- ข้อ 11 ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของโรงเรียน หรือเป็นข้อมูลของบุคคลภายนอก
- ข้อ 12 ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของโรงเรียนห้วยกรดวิทยา ถือเป็นทรัพย์สินของโรงเรียน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บริหารโรงเรียน
- ข้อ 13 ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงเรียน หรือข้อมูลของ ผู้รับบริการ หากเกิดการสูญหายโดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย
- ข้อ 14 ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล
- ข้อ 15 ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาเพิ่มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาตห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงข้อมูลด้านเทคโนโลยีสารสนเทศของโรงเรียน โดยไม่ได้รับอนุญาตจากผู้บริหารโรงเรียนหรือผู้ที่ได้รับมอบหมาย

หมวด 4

การรักษาความปลอดภัยของการสำรองข้อมูล (Backup Policy)

- ข้อ 17 จัดทำสำเนาข้อมูลด้านเทคโนโลยีสารสนเทศเก็บไว้ โดยจัดเรียงลำดับข้อมูลของโรงเรียนตามความจำเป็นจากมากไปหาน้อย
- ข้อ 18 มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้องในแต่ละระบบงาน
- ข้อ 19 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการติดฉลากบนสื่อเก็บข้อมูลนั้นให้สามารถ แสดงถึงระบบงาน วันที่ เวลาที่สำรองข้อมูล จำนวนหน่วยของข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลได้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่ที่ปลอดภัย และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ
- ข้อ 20 ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ ภายในระยะเวลาที่เหมาะสม

หมวด 5

ซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

- ข้อ 21 โรงเรียนห้วยกรดวิทยาได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่โรงเรียนห้วยกรดวิทยาอนุญาตให้ใช้งานหรือที่โรงเรียนห้วยกรดวิทยามีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และโรงเรียนห้วยกรดวิทยาห้ามไม่ให้ ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิด ลิขสิทธิ์ โรงเรียนห้วยกรดวิทยาถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว
- ข้อ 22 ซอฟต์แวร์ (Software) ที่โรงเรียนห้วยกรดวิทยาได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

หมวด 6

การป้องกันโปรแกรมไม่ประสงค์ดี (Preventing MalWare)

- ข้อ 23 คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti virus) ตามที่ ผู้บริหารโรงเรียนกำหนดให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนาระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้บริหารโรงเรียนก่อน
- ข้อ 24 บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง
- ข้อ 25 ผู้จัดการ/ผู้ดูแลระบบงานต้องทำการปรับปรุงโปรแกรมป้องกันไวรัสคอมพิวเตอร์และปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

- ข้อ 26 ผู้ใช้งานต้องพึงระวังไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้จัดการ/ผู้ดูแลระบบ ทราบ
- ข้อ 27 เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้า สู่ระบบ เครือข่าย และต้องแจ้งแก่ผู้จัดการ/ผู้ดูแลระบบ
- ข้อ 28 ห้ามลักลอบเปลี่ยนแปลง ลบทิ้ง โปรแกรมป้องกันไวรัสคอมพิวเตอร์ ในระบบของโรงเรียนห้วยกรดวิทยา โดยไม่ได้รับอนุญาตจากผู้บริหารโรงเรียนหรือผู้ที่ได้รับมอบหมาย
- ข้อ 29 ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ ทรัพย์สินของโรงเรียนห้วยกรดวิทยา

หมวด 7

การรักษาความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(Network and Server Policy)

- ข้อ 30 เครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องต้องตั้งอยู่ที่ปลอดภัยและป้องกันบุคคลเข้าถึงโดยไม่ได้รับ อนุญาต เว้นแต่ได้รับอนุญาตจากผู้จัดการ/ผู้ดูแลระบบ (System Administrator)
- ข้อ 31 ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่ จะได้รับ อนุญาตจากผู้จัดการ/ผู้ดูแลระบบ
- ข้อ 32 ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมต่อเข้าเครือข่าย เพื่อการประกอบธุรกิจส่วนบุคคล
- ข้อ 33 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัด เส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้จัดการ/ผู้ดูแลระบบ
- ข้อ 34 โรงเรียนห้วยกรดวิทยาต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้ อย่างมีประสิทธิภาพ ดังต่อไปนี้
 - (1) ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบ เครือข่ายที่ได้รับอนุญาต เท่านั้น
 - (2) ระบบเครือข่ายทั้งหมดของโรงเรียนห้วยกรดวิทยาที่มีการเชื่อมต่อไปยังระบบเครือข่าย อื่นๆ ภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการ ตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย
 - (3) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบ เครือข่ายของ หน่วยงานในลักษณะที่ผิดปกติ

(4) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบัน อยู่เสมอ

(5) การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้จัดการ/ ผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ข้อ 35 โรงเรียนห้วยกรดวิทยาต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ 36 โรงเรียนห้วยกรดวิทยากำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

(1) บุคคลจากหน่วยงานภายนอกโรงเรียนห้วยกรดวิทยาที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของโรงเรียนห้วยกรดวิทยาจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้บริหารโรงเรียนห้วยกรดวิทยา

(2) วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการ อนุญาตจากผู้บริหารโรงเรียนห้วยกรดวิทยา

(3) การเข้าสู่ระบบจากระยะไกลผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็น ในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

หมวด 8

การรักษาความปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)

ข้อ 37 ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของโรงเรียนห้วยกรดวิทยา เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจ กระทบกระเทือนหรือเป็นภัยต่อการรักษาความต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ 38 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่าง เป็นทางการผ่านระบบอินเทอร์เน็ต

ข้อ 39 รมัถระวังการดาวนโโหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวนโโหลด การอัปเดต (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ 40 หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์เพื่อป้องกันการ เข้าใช้งานโดยบุคคลอื่น

หมวด 9

การรักษาความปลอดภัยของอีเมล (E-mail Policy)

- ข้อ 41 ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงานโดยยื่นคำขอกับผู้จัดการ/ผู้ดูแลระบบ
- ข้อ 42 เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และเมื่อมีการเข้าสู่ระบบในครั้งนั้น ควรเปลี่ยนรหัสผ่าน (Password) โดยทันที
- ข้อ 43 ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์
- ข้อ 44 ควรเปลี่ยนรหัสผ่าน (Password) ทุก 6 เดือน
- ข้อ 45 ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

ประกาศ ณ วันที่ 18 กุมภาพันธ์ พ.ศ. 2562



(นางสาวสุวาริตรี ภูเปี่ยมสินธุ์)

ผู้อำนวยการโรงเรียนห้วยกรดวิทยา

นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. 2562

(Information Security Policy)

ที่ปรึกษา

นางสาวสุวาริศิริ ภูเปี่ยมสินธุ์	ผู้อำนวยการโรงเรียนห้วยกรดวิทยา
นายพุ่ม ก้อนทอง	หัวหน้ากลุ่มบริหารงานงบประมาณ
นางวัฒนา สุนิรมิต	หัวหน้ากลุ่มบริหารงานบุคคล
นางนงนุช จันทร์สวาท	หัวหน้ากลุ่มบริหารงานวิชาการ
นายมานพ พลับเที่ยง	หัวหน้ากลุ่มบริหารงานทั่วไป

คณะทำงาน

คณะกรรมการจัดทำร่างนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. 2562

รวบรวม/วิเคราะห์ข้อมูล/รูปเล่ม

นายสุเมธ ราชประชุม หัวหน้ากลุ่มงานระบบไอซีที

ปีที่พิมพ์ กุมภาพันธ์ 2562