แนวปฏิบัติสำหรับการบริหารจัดการเว็บไซต์ของหน่วยงานภายใต้สังกัดกรมราชทัณฑ์

การแต่งตั้งหรือเปลี่ยนแปลงผู้ดูแลระบบ (Admin) ของหน่วยงาน

1. ให้ผู้บัญชาการเรือนจำ/ผู้อำนวยการกอง มอบหมายเจ้าหน้าที่ผู้ปฏิบัติหน้าที่ดังนี้
   - ผู้ดูแลระบบ (Admin) จำนวน 2 ราย
   - ผู้ใช้งานสำหรับลงประกาศ/ข่าวสารในเว็บไซต์หลักของกรมราชทัณฑ์ จำนวน 2 ราย

   โดยเจ้าหน้าที่จะต้องเป็นข้าราชการ หรือพนักงานราชการ เท่านั้น
2. ดำเนินการกรอก **แบบฟอร์มการสมัครผู้ดูแลระบบเว็บไซต์ของหน่วยงาน** และจัดส่งหนังสือมายังกรมราชทัณฑ์ โดยเรียน ผู้อำนวยการกองยุทธศาสตร์และแผนงาน
3. หากมีการเปลี่ยนแปลงรายชื่อผู้ดูแลระบบ (Admin) ให้หน่วยงานดำเนินการแจ้งการเปลี่ยนแปลงผู้ได้รับมอบหมายปฏิบัติหน้าที่แทนผู้ดูแลระบบ (Admin) โดยรายงานตาม **แบบฟอร์มการสมัครผู้ดูแลระบบเว็บไซต์หน่วยงาน** โดยเรียน ผู้อำนวยการกองยุทธศาสตร์และแผนงาน

การจัดการโครงสร้างของเว็บไซต์และการใช้งาน

1. กรมราชทัณฑ์เป็นผู้กำหนดโดเมนและที่อยู่ของเว็บไซต์ให้หน่วยงานในสังกัด
2. กรมราชทัณฑ์จะจัดสรรพื้นที่ใช้งานสำหรับเว็บไซต์ของหน่วยงาน ขนาดไม่เกิน 5 GB หากมีความจำเป็นต้องการขอใช้พื้นที่มากกว่าที่กรมราชทัณฑ์กำหนด ให้ดำเนินการแจ้งเหตุผลความจำเป็นตาม **แบบฟอร์มการขอใช้พื้นที่เครื่องคอมพิวเตอร์แม่ข่ายของกรมราชทัณฑ์**
3. ห้ามแก้ไขปรับปรุง โครงสร้างของเว็บไซต์ และติดตั้งปลั๊กอินเพิ่มเติม โดยที่ไม่ได้รับอนุญาตจากกรมราชทัณฑ์
4. ห้ามอัปโหลดภาพหรือข้อมูลที่ไม่เหมาะสม รวมถึงข้อมูลส่วนบุคคลที่ไม่ได้รับการยินยอมให้เปิดเผย
5. ให้หน่วยงานจัดเก็บเอกสารไว้บนระบบ Google Drive จากนั้นให้คัดลอกลิงก์ของเอกสารดังกล่าวมาเผยแพร่ยังเว็บไซต์ของหน่วยงาน เพื่อเป็นการประหยัดพื้นที่การจัดเก็บข้อมูลของเว็บไซต์
6. เจ้าหน้าที่ผู้รับผิดชอบในการนำข้อมูลเข้าสู่เว็บไซต์จะต้องตรวจความสมบูรณ์ของข้อมูลและความถูกต้องเสมอ และแจ้งผู้รับผิดชอบการให้ข้อมูล หรือหน่วยงานเจ้าของเรื่อง ตรวจสอบเมื่อดำเนินการแล้วเสร็จ
7. เมื่อพบปัญหาในการดำเนินการอัปโหลดข้อมูลขึ้นเว็บไซต์ ให้แจ้งผู้ดูแลระบบของที่ศูนย์เทคโนโลยีสารสนเทศ เพื่อดำเนินการตรวจสอบ และแก้ไข ภายในระยะเวลา 15 – 30 วัน
8. ผู้รับผิดชอบในการอัปโหลดหรือนำเข้าข้อมูลลงบนเว็บไซต์ ต้องดำเนินการตรวจสอบความถูกต้องและปรับปรุงข้อมูลให้เป็นปัจจุบันอยู่เสมอ และขอความเห็นชอบจากผู้บังคับบัญชาก่อนดำเนินการเผยแพร่ข้อมูลผ่านเว็บไซต์ และต้องจัดเก็บข้อมูลสำรองไว้ทุกครั้งเพื่อประโยชน์ในการบริหารจัดการข้อมูลและการกู้คืนข้อมูล
9. การอัปโหลดเนื้อหาลงบนเว็บไซต์ ผู้รับผิดชอบควรเลือกใช้คำอธิบายหรือข้อความบรรยายที่มีความถูกต้องเหมาะสม และไม่ละเมิดลิขสิทธิ์ หากมีความจำเป็นต้องนำเนื้อหาที่มีเจ้าของลิขสิทธิ์มาเผยแพร่ ต้องระบุแหล่งที่มาหรือข้อมูลอ้างอิงอย่างชัดเจนทุกครั้ง เพื่อให้เป็นไปตามหลักเกณฑ์ทางกฎหมาย
10. ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 อย่างเคร่งครัด เพื่อป้องกันไม่ให้เกิดความเสียหายและลดโอกาศที่จะเกิดความเสียหายแก่ทางราชการ

11. ผู้ดูแลเว็บไซต์จะต้องตรวจสอบ ปรับปรุงและพัฒนาเว็บไซต์ ตามมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานเว็บไซต์ภาครัฐ เวอร์ชัน 3.0 เพื่อเป็นแนวทางในการพัฒนาเว็บไซต์ให้สอดคล้องกับเว็บไซต์หลักของกรมราชทัณฑ์

การตั้งรหัสผ่านและความปลอดภัยของข้อมูล

1. ห้ามหน่วยงานภายในสังกัดกรมราชทัณฑ์ทำเว็บไซต์หน่วยงานเอง โดยใช้พื้นบนเครื่องแม่ข่ายภายนอกที่กรมราชทัณฑ์ไม่ได้กำหนด
2. กำหนด ‘รหัสผ่าน (password)’ จำนวนไม่น้อยกว่า 12 หลักขึ้นไป โดยจะต้องประกอบด้วย
    1) ตัวพิมพ์ใหญ่ (A–Z)
    2) ตัวพิมพ์เล็ก (a–z)
    3) ตัวเลข (0–9)
    4) อักขระพิเศษ (@#*_&)
3. หลีกเลี่ยงการตั้งรหัสผ่านที่เป็นรูปแบบ ‘แพทเทิน (Pattern)’ ดังนี้
    1) ตัวอักษรพิมพ์ใหญ่ 1 ตัว + ตัวอักษรพิมพ์เล็ก 5 ตัว ตัวเลข 3 หลัก เช่น Docdoc123
    2) ตัวอักษรพิมพ์ใหญ่ 1 ตัว + ตัวอักษรพิมพ์เล็ก 6 ตัว ตัวเลข 2 หลัก เช่น Correct12
    3) ตัวอักษรพิมพ์ใหญ่ 1 ตัว + ตัวอักษรพิมพ์เล็ก 3 ตัว ตัวเลข 5 หลัก เช่น Ddoc12345
4. ไม่กำหนดรหัสผ่านที่คาดเดาได้ง่าย
    1) วัน/เดือน/ปี เกิด
    2) เบอร์โทรศัพท์ส่วนตัว
    3) ชื่อจริงหรือชื่อเล่น
    4) ชื่อหน่วยงาน
    5) เลขบัตรประจำตัวประชาชน
    6) คำที่ใช้ในพจนานุกรม หรือตามแป้นพิมพ์ เช่น qwerty,word,window เป็นต้น
    7) ไม่ควรใช้รหัสผ่านเดียวกันซ้ำๆ สำหรับหลายระบบ เช่น อีเมลส่วนตัว ระบบงานของหน่วยงาน หรือบริการทางการเงิน (ระบบธนาคารออนไลน์) เพื่อป้องกันความเสี่ยงจากการถูกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หากรหัสผ่านใดรหัสผ่านหนึ่งถูกเปิดเผยหรือรั่วไหล
5. ห้ามส่งรหัสผ่าน ผ่านทางอีเมล ข้อความโต้ตอบ (Chat) หรือช่องทางการสื่อสารอื่นใดที่ขาดความปลอดภัยในการเข้ารหัสหรือการป้องกันข้อมูล เพื่อป้องกันความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
6. ไม่ควรจดจำรหัสผ่านผ่านเว็บเบราว์เซอร์ทุกประเภท เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
7. ผู้ดูแลระบบต้องทำการเปลี่ยนรหัสผ่าน ของตนเองและผู้ใช้งานภายใต้การกำกับดูแล ทุกๆ 90 วัน
8. ผู้ใช้งานระบบ หรือผู้ดูแลระบบ ต้องออกจากระบบทุกครั้งหลังการงานเสร็จสิ้น