แนวปฏิบัติในการควบคุมสิทธิ์การเข้าถึงข้อมูลที่สำคัญ (Access Control)
(กรมราชทัณฑ์ พ.ศ. ๒๕๖๘)

ศูนย์เทคโนโลยีสารสนเทศ
กองยุทธศาสตร์และแผนงาน

แนวปฏิบัติในการควบคุมสิทธิ์การเข้าถึงข้อมูลที่สำคัญ (Access Control) กรมราชทัณฑ์ พ.ศ. ๒๕๖๘

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีผลบังคับใช้ เพื่อป้องกัน ความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังนั้นเพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที มิให้เกิดผลกระทบต่อความมั่นคง ปลอดภัยทางด้านสารสนเทศ กรมราชทัณฑ์

กรมราชทัณฑ์ จึงได้จัดทำแนวทางปฏิบัติในการควบคุมสิทธิ์การเข้าถึงข้อมูลที่สำคัญ (Access Control) เพื่อให้สอดคล้องกับมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยจำเป็นอย่างยิ่งที่ต้องได้รับความร่วมมือจากผู้ที่เกี่ยวข้อง จึงกำหนดแนวปฏิบัติ เพื่อใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ส่งผลให้การใช้งานระบบสารสนเทศ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ และป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่ถูกต้องซึ่งอาจส่งผลให้เกิดภัยคุกคามในลักษณะต่าง ๆ ต่อระบบสารสนเทศของหน่วยงาน กองยุทธศาสตร์และแผนงาน จึงได้จัดทำแนวปฏิบัติในการควบคุมสิทธิ์การเข้าถึงข้อมูลที่สำคัญ (Access Control) ขึ้นเพื่อเผยแพร่ให้บุคลากร และบุคคลภายนอกที่ปฏิบัติงานร่วมกับกรมราชทัณฑ์ ได้รับทราบและให้ความร่วมมือปฏิบัติตามอย่างเคร่งครัดต่อไป ตามรายละเอียด ดังนี้

๑. ระเบียบการใช้สารสนเทศภายในกรมราชทัณฑ์ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

๑.๑ กรมราชทัณฑ์เป็นหน่วยงานของรัฐในสังกัดกระทรวงยุติธรรม ซึ่งปฏิบัติราชการภายใต้บังคับแห่งกฎหมายไทย ดังนั้น การใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อทางเครือข่ายอินเทอร์เน็ตของกรมราชทัณฑ์ จะต้องเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นที่เกี่ยวข้อง

๑.๒ กรมราชทัณฑ์ไม่ส่งเสริมหรือยินยอมให้เจ้าหน้าที่ของหน่วยงานกระทำการใด ๆ อันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นที่เกี่ยวข้อง

๑.๓ ระบบคอมพิวเตอร์และอุปกรณ์เครือข่ายถือเป็นทรัพย์สินของหน่วยงาน ห้ามผู้ไม่ได้รับอนุญาตหรือผู้ที่ไม่เกี่ยวข้องใช้งานโดยมิได้รับอนุญาต หากผู้ใดกระทำการใด ๆ เป็นการบุกรุกเขตหวงห้ามหรือพยายามบุกรุกเข้าสู่ระบบเครือข่าย ถือเป็นการละเมิดตามกฎหมาย ต้องได้รับโทษตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นที่เกี่ยวข้อง

๑.๔ สิทธิ์ในการเข้าถึงการใช้สารสนเทศ เป็นไปตามบทบาทหน้าที่ที่เกี่ยวข้องหรือได้รับมอบหมายจากผู้บังคับบัญชา ไม่อนุญาตให้ผู้ที่ไม่เกี่ยวข้องกับสารสนเทศ หรือในส่วนที่ไม่เกี่ยวข้องกับตนเข้าใช้งาน

๑.๕ การยืมทรัพย์สินสารสนเทศจะต้องทำตามขั้นตอนการยืม และเมื่อสิ้นสุดการใช้งานหรือสิ้นสุดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง จะต้องคืนทรัพย์สินตามขั้นตอนการคืนทรัพย์สิน

๑.๖ การทำลายอุปกรณ์หรือสื่อบันทึกข้อมูล หรือสารสนเทศ ต้องทำตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการพัสดุ พ.ศ. ๒๕๖๑

๑.๗ เครื่องคอมพิวเตอร์ และอุปกรณ์ประกอบที่สำคัญ จะต้องมีการกำหนดรหัสผ่าน (Password) ที่มีความยาวอย่างน้อย ๖–๘ ตัว เพื่อควบคุมการเข้าถึงและเพื่อป้องกันการเข้าถึงข้อมูล สำนักงาน โดยไม่ได้รับอนุญาต

๒. แนวปฏิบัติ

๒.๑ ระดับชั้นการเข้าถึง แบ่งเป็น ๓ ระดับ ดังนี้

๒.๑.๑ ระดับชั้นผู้ดูแลระบบ (Administrator)

๒.๑.๒ ระดับชั้นผู้อนุมัติ (Approver)

๒.๑.๓ ระดับชั้นผู้ใช้งาน (User)

๒.๒ การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศกำหนด ดังนี้

๒.๒.๑ ผู้ดูแลระบบ (Administrator) กำหนดสิทธิ์ ตรวจสอบสิทธิ์ ทบทวนสิทธิ์ และบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ

๒.๒.๒ ผู้อนุมัติ (Approver) อนุมัติสิทธิ์ให้ผู้ใช้งานตามภารกิจ เพื่อให้สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ เฉพาะในส่วนที่ได้รับมอบหมาย ตามความเป็นจำในการใช้งาน

๒.๒.๓ ผู้ใช้งาน (User) ตามสิทธิ์การเข้าถึงข้อมูลที่กำหนด

๒.๓ เกณฑ์ในการอนุญาตการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ดังนี้

๒.๓.๑ สิทธิ์ของผู้ดูแลระบบ (Administrator) แต่ละระบบสารสนเทศ ดังนี้

- อ่านข้อมูล
- ป้อนข้อมูล
- แก้ไข

๒.๓.๒ สิทธิ์ของผู้อนุมัติ (Approver) แต่ละระบบสารสนเทศ ดังนี้

- อ่านข้อมูล
- อนุมัติ

๒.๓.๓ สิทธิ์ของผู้ใช้งาน (User) แต่ละระบบสารสนเทศ ดังนี้

- อ่านอย่างเดียว
- ป้อนข้อมูล
- แก้ไข

ตารางที่ ๑ สิทธิ์ของผู้ใช้งาน

ระบบ	**ผู้ใช้งาน (User)** (ป้อนข้อมูล/อ่านข้อมูล)	**ผู้อนุมัติ (Approver)** (อนุมัติ)	**ผู้ดูแลระบบ** (Administrator) (สร้างข้อมูล/แก้ไข)
ระบบข้อมูลผู้ต้องขัง	เจ้าหน้าที่ในสังกัดกรมราชทัณฑ์ที่ได้รับมอบหมายให้ปฏิบัติงานด้านข้อมูลในระบบข้อมูลผู้ต้องขัง	ผู้บังคับบัญชา ได้แก่ - ผู้อำนวยการกอง - ผู้อำนวยการกลุ่มงาน	นักวิชาการคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศกองยุทธศาสตร์และแผนงาน

ทั้งนี้ ขอให้เจ้าหน้าที่ในสังกัดกรมราชทัณฑ์ถือปฏิบัติตามแนวทางการควบคุมสิทธิ์การเข้าถึงข้อมูลที่สำคัญ (Access Control) ถือปฏิบัติโดยเคร่งครัด