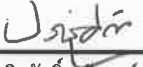
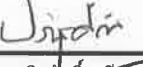



	นโยบายการควบคุมการเข้าถึง (Access Control Policy)	รหัสเอกสาร :	ICIT-PC-27001-01
		แก้ไขครั้งที่ :	00
		วันที่บังคับใช้ :	28 พฤษภาคม 2562

สำหรับ
สำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

การอนุมัติเอกสาร

	ผู้เรียบเรียง/ ผู้จัดทำ	ผู้ตรวจสอบ/ ผู้ทบทวน	ผู้อนุมัติ
ลงนาม	 (ผศ.ดร. ประเสริฐศักดิ์ เตียววงศ์สมบัติ)	 (ผศ.ดร. ประเสริฐศักดิ์ เตียววงศ์สมบัติ)	 (รศ. ดร.ชูพันธุ์ รัตนโกศา)
ตำแหน่ง	คณะทำงาน สำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ	รองผู้อำนวยการฝ่ายบริหาร สำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ	ผู้อำนวยการ สำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ประวัติการแก้ไข

ครั้งที่แก้ไข	วันที่บังคับใช้	รายละเอียดการแก้ไข
00	28 พฤษภาคม 2562	จัดทำเอกสารครั้งแรก

รายการเผยแพร่เอกสาร

รหัสเอกสาร	รายชื่อเอกสาร	รายชื่อผู้รับเอกสาร	แก้ไขครั้งที่	ระยะเวลาจัดเก็บเอกสาร
	การควบคุมการเข้าถึง (Access Control Policy)	กลุ่ม Management	00	3 ปี
		กลุ่ม ISMR		
		กลุ่ม Service		
		กลุ่ม DCC		

Contents

1	วัตถุประสงค์.....	3
2	ขอบเขตการบังคับใช้.....	3
3	คำจำกัดความ.....	3
4	นโยบายควบคุมการเข้าถึง (Access Control Policy)	3
	4.1 การกำหนดสิทธิ์บน Access Right Matrix.....	4
	4.2 การทบทวนสิทธิ์บน Access Right Matrix.....	4
	4.3 การเปลี่ยนแปลงสิทธิ์บน Access Right Matrix.....	4
5	กระบวนการลงทะเบียนและการเพิกถอนทะเบียนผู้ใช้งาน (User Registration and De-registration Procedure).....	5
	5.1 ขอบเขตการดำเนินงาน.....	5
	5.2 การดำเนินการขอใช้สิทธิ์.....	5
	5.3 การดำเนินการขอเปลี่ยนแปลงสิทธิ์.....	5
	5.4 การดำเนินการขอเพิกถอนสิทธิ์.....	5
	5.5 การจัดส่งรหัสผ่าน.....	6
	5.6 การทบทวนสิทธิ์.....	6
6	นโยบายบริหารจัดการรหัสผ่าน (Password Management Policy)	6
7	ภาคผนวก.....	6

1 วัตถุประสงค์

เพื่อใช้เป็นนโยบาย ในการควบคุมและป้องกันการเข้าถึง การเปิดเผย และการแก้ไขสารสนเทศและระบบสารสนเทศขององค์กร โดยมีได้รับอนุญาต โดยมีการกำหนดสิทธิการเข้าถึงระบบนั้นๆ โดยได้จัดทำขึ้นตามข้อกำหนดของมาตรฐานระบบจัดการ ISO 27001:2013 ของสำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ข้อกำหนดจัดการ ISO 27001:2013 ที่เกี่ยวข้อง ประกอบด้วย

- A.9.1 การควบคุมการเข้าถึงให้เป็นไปตามความต้องการทางธุรกิจ (Business Requirements of Access Control)
- A.9.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
- A.9.3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
- A.9.4 การควบคุมการเข้าถึงระบบ (System and Application Access Control)

2 ขอบเขตการบังคับใช้

สำหรับเป็นขั้นตอนการปฏิบัติเฉพาะภายในสำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

3 คำจำกัดความ

อ้างอิงตามเอกสาร Terms and definitions

4 นโยบายควบคุมการเข้าถึง (Access Control Policy)

เป็นนโยบายหลักในการควบคุมการเข้าถึงระบบต่างๆ ทั้งการเข้าถึง Operation System และ Application ของระบบ ดังต่อไปนี้

No	ระบบ / พื้นที่	Operating System	Application	Console
1	Core Switch 9500	Yes	N/A	Yes
2	Router 7606	Yes	N/A	Yes
3	Router 902	Yes	N/A	Yes
4	Load Balance F5	Yes	Yes	Yes
5	Firewall Paloalto PA-5050	Yes	Yes	Yes
6	IPS Cisco FirePower	N/A	Yes	N/A
7	PRTG	Yes	Yes	N/A
8	Team Drive : DCC Documents	N/A	Yes	N/A
9	Log System (ArcSight appliance)	N/A	Yes	Yes
10	VPN	N/A	Yes	Yes

ทุกระบบงานตามตารางข้างต้น จะต้องมีการกำหนดสิทธิในการเข้าถึง Operating System และ Application ของระบบ บน Access Right Matrix โดยแบ่งวิธีการควบคุมสิทธิบน Access Right Matrix ดังนี้

- 4.1 การกำหนดสิทธิบน Access Right Matrix
- 4.2 การทบทวนสิทธิบน Access Right Matrix
- 4.3 การเปลี่ยนแปลงสิทธิบน Access Right Matrix

4.1 การกำหนดสิทธิ์บน Access Right Matrix

ทุกระบบงานตามตารางข้างต้น จะต้องมีการกำหนดสิทธิ์ในการเข้าถึง Operating System และ Application ของระบบบน Access Right Matrix โดยการกำหนดสิทธิ์ดังกล่าว ให้เจ้าของระบบ เป็นผู้ตัดสินใจ โดยคำนึงถึงความจำเป็นและความเหมาะสมในการปฏิบัติงานของแต่ละบุคคล

การกำหนดสิทธิ์การเข้าถึงระบบต่างๆ บน Access Right Matrix กำหนดสิทธิ์การเข้าถึงระบบต่างๆ ตามรายบุคคล โดยแต่ละบุคคล มีสิทธิ์ในการเข้าถึงแต่ละระบบได้อย่างใดอย่างหนึ่งใน 3 ระดับ คือ Super User (S), User (U) และ Admin (A) โดยสามารถดูตัวอย่างตาราง Access Right Matrix ได้ในภาคผนวกของเอกสารนี้ ทั้งนี้หากระบบบางระบบ มีระดับการเข้าถึงมากกว่า 3 ระดับ ให้เจ้าของระบบสามารถกำหนดสิทธิ์การเข้าถึงในระดับอื่นๆ เพิ่มเติมได้

Access Right Matrix ที่ได้รับการกำหนดสิทธิ์เรียบร้อยแล้ว ให้ผู้รับผิดชอบระบบนำไปกำหนดสิทธิ์ในการเข้าถึงระบบจริงๆ ต่อไป

4.2 การทบทวนสิทธิ์บน Access Right Matrix

เจ้าของระบบ ต้องทำการทบทวนสิทธิ์การเข้าถึงระบบต่างๆ โดยเปรียบเทียบสิทธิ์บน Access Right Matrix กับสิทธิ์การเข้าถึงที่ถูกตั้งค่าไว้ในระบบ และเก็บหลักฐานการทบทวน จัดทำเป็นรายงานส่งให้ Team Leader รับทราบและอนุมัติทุก 6 เดือน

4.3 การเปลี่ยนแปลงสิทธิ์บน Access Right Matrix

การเพิ่ม ลด หรือเปลี่ยนแปลงสิทธิ์ หรือเปลี่ยนแปลง User ของระบบต่างๆ เจ้าของระบบจะต้องดำเนินการตามขั้นตอนที่ระบุไว้ใน User Registration and De-registration Procedure

หลังจากผ่านกระบวนการ User Registration and De-registration Procedure ให้ผู้รับผิดชอบระบบนำข้อมูลการเปลี่ยนแปลงสิทธิ์ดังกล่าว ไป Configure สิทธิ์ในการเข้าถึงจริงบนระบบต่าง และส่งข้อมูลการเปลี่ยนแปลงสิทธิ์ให้ทีม DCC นำไปปรับปรุงแก้ไขบนเอกสาร Access Right Matrix

การเปลี่ยนแปลงสิทธิ์ในการเข้าถึงระบบต่างๆ ต้องผ่านกระบวนการ User Registration and De-registration Procedure และปรับปรุงข้อมูลบนเอกสาร Access Right Matrix โดยไม่มีข้อยกเว้น

5 กระบวนการลงทะเบียนและการเพิกถอนทะเบียนผู้ใช้งาน (User Registration and De-registration Procedure)

กระบวนการนี้ มีจุดประสงค์เพื่อให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนและให้สิทธิผู้ใช้งาน (User Registration) การเปลี่ยนแปลงข้อมูลและสิทธิของผู้ใช้งาน (User Modification) และ การเพิกถอนการลงทะเบียนและสิทธิผู้ใช้งาน (User De-Registration)

5.1 ขอบเขตการดำเนินงาน

ในการระบุผู้กำหนดสิทธิ์การเข้าถึง แต่ละระบบหรือพื้นที่ ให้พิจารณาตารางดังต่อไปนี้

No	ระบบ / พื้นที่	ผู้อนุมัติ	ผู้ได้รับมอบหมาย
1	Core Switch 9500	Team leader	Admin
2	Router 7606	Team leader	Admin
3	Router 902	Team leader	Admin
4	Load Balance F5	Team leader	Admin
5	Firewall Paloalto PA-5050	Team leader	Admin
6	IPS Cisco FirePower	Team leader	Admin
7	PRTG	Team leader	Admin
8	Team Drive : DCC Documents	Team leader	Admin
9	Log System (ArcSight appliance)	Team leader	Admin
10	VPN	Team leader	Admin

โดยการกำหนดสิทธิ์การเข้าถึงของระบบและพื้นที่ต่างๆให้ใช้แบบฟอร์มลงทะเบียนผู้ใช้ User Registration De-Registration Form

5.2 การดำเนินการขอใช้สิทธิ์

ให้ผู้ร้องขอ ดำเนินการกรอกแบบฟอร์มลงทะเบียนผู้ใช้ โดยเลือกประเภทคำร้องเป็น “การเพิ่มสิทธิ” โดยให้ผู้ดูแลระบบ เป็นผู้กำหนดรายการสิทธิ์ตามความเหมาะสม จากนั้นส่งแบบฟอร์มให้ เจ้าของระบบ หรือ Team leader เพื่อขออนุมัติ

ในการให้สิทธิ ต้องระบุระยะเวลาการอนุญาตที่แน่นอน โดยให้ระบุวันที่สิ้นสุดลงในแบบฟอร์มลงทะเบียนผู้ใช้ด้วยทุกครั้ง หากต้องการแก้ไขหรือขยายระยะเวลาให้ดำเนินการตามการร้องขอเปลี่ยนแปลงสิทธิ ในแบบฟอร์มลงทะเบียนผู้ใช้ อีกครั้ง

5.3 การดำเนินการขอเปลี่ยนแปลงสิทธิ

ให้ผู้ร้องขอ ดำเนินการกรอกแบบฟอร์มลงทะเบียนผู้ใช้ โดยเลือกประเภทคำร้องเป็น “การเปลี่ยนแปลงสิทธิ” พร้อมทั้งระบุสิทธิที่ต้องการและเหตุผลในช่องโปรดระบุรายละเอียดหรือสาเหตุ โดยให้เจ้าของระบบเป็นผู้พิจารณาสิทธิ์ที่ต้องการเปลี่ยนแปลง จากนั้นส่งแบบฟอร์มให้ เจ้าของระบบ หรือ Team leader เพื่อขออนุมัติ

5.4 การดำเนินการขอเพิกถอนสิทธิ์

- ผู้ร้องขอ หรือผู้ที่ได้รับมอบหมาย ดำเนินการกรอกแบบฟอร์มลงทะเบียนผู้ใช้ โดยเลือกประเภทคำร้องเป็น “การลบสิทธิ” ตามรายการสิทธิ์ที่ต้องมีการเพิกถอน
- เจ้าของระบบ เป็นผู้พิจารณาในการเพิกถอนสิทธิ จากนั้นส่งแบบฟอร์ม ให้ เจ้าของระบบ หรือ Team leader เพื่อขออนุมัติ
- เจ้าของระบบ ดำเนินการเพิกถอนสิทธิ์ผู้ใช้งานที่ได้มีการร้องขอ โดยจะต้องดำเนินการให้แล้วเสร็จภายใน 1 วัน ภายหลังจากวันที่มีคำสั่งอนุมัติให้ลาออกหรือโยกย้ายอย่างเป็นทางการ

5.5 การจัดส่งรหัสผ่าน

หลังจากการลงทะเบียนผู้ใช้ ตามสิทธิ์ที่ได้มีการระบุในแบบฟอร์มลงทะเบียนผู้ใช้ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องจัดส่ง User Account (User ID และรหัสผ่าน) ให้แก่ผู้ร้องขอ โดยจัดส่งทาง email และแยกจัดส่ง User ID และรหัสผ่าน ออกเป็น 2 ครั้ง

ผู้ดูแลระบบ จะต้องบังคับให้มีการเปลี่ยนรหัสผ่านทันทีที่มีการใช้งาน และแจ้งให้ผู้ร้องขอให้ดำเนินการดังกล่าว และหากมีความจำเป็นต้อง Reset รหัสผ่าน ผู้ดูแลระบบต้องมั่นใจได้ว่าผู้ร้องขอเป็นเจ้าของรหัสนั้นจริง

5.6 การทบทวนสิทธิ์

ผู้ดูแลระบบ จะต้องมีการทบทวนรายชื่อและสิทธิ์ของผู้ใช้งาน ตามรายละเอียดที่ระบุไว้ใน Access Control Policy

6 นโยบายบริหารจัดการรหัสผ่าน (Password Management Policy)

ผู้ใช้งานต้องปฏิบัติตามดังนี้

1. ต้องไม่เปิดเผยรหัสผ่านกับผู้อื่น รวมถึงผู้บริหาร และ admin
2. การสร้างรหัสผ่านสำหรับผู้ใช้งาน
 - รหัสผ่านควรมีอย่างน้อย 8 ตัวอักษร ยกเว้นกรณีที่มีข้อจำกัดทางเทคนิค
 - รหัสผ่านควรประกอบด้วยอักษรตัวใหญ่ อักษรตัวเล็ก ตัวเลข และอักขระพิเศษ เช่น \$, ! (*) / \ ผสมกัน
 - รหัสผ่านใหม่ควรมีอย่างน้อย 6 ตัวอักษรที่ไม่ตรงกับตัวอักษรในรหัสผ่านเก่าที่จะเปลี่ยน
 - รหัสผ่านไม่ควรจะให้ผู้อื่นคาดเดาได้ง่ายหรือคาดเดาได้จากคำต่างๆที่พบในพจนานุกรม ชื่อบริษัท ตำแหน่งทางภูมิศาสตร์ ตัวละครในนิยายที่รู้จักกันทั่วไปจากหนังสือ ภาพยนตร์ และอื่นๆ
 - รหัสผ่านไม่ควรตั้งจากข้อมูลส่วนตัวของผู้ใช้งาน
3. เปลี่ยนรหัสผ่านเมื่อพบว่า มีผู้อื่นนำรหัสผ่านไปใช้งาน
4. ผู้ใช้งานควรเปลี่ยนรหัสผ่านเริ่มต้นทันทีหลังจากสามารถเข้าใช้งานระบบได้ในครั้งแรก
5. รหัสผ่านต้องถูกกำหนดให้หมดอายุทุก 90 วันเพื่อให้ผู้ใช้งานทำการเปลี่ยนรหัสผ่านใหม่
6. ระบบต้องบันทึกรหัสผ่านที่เขี่ย้นหลังไป 5 ครั้ง รหัสผ่านที่ตั้งใหม่ต้องไม่ซ้ำกับรหัสผ่านใดๆของ 5 ครั้งก่อน

7 ภาคผนวก

ตัวอย่างเอกสาร Access Right Matrix

Operating System	System 1	System 2	System n
Staff 1	A	U	n/a	n/a	n/a
Staff 2	n/a	G	A	n/a	U
...					
...					
Staff n					

A = Admin, U = User, S = Super User

Application	System 1	System 2	System n
Staff 1	A	U	n/a	n/a	n/a
Staff 2	n/a	G	A	n/a	U
...					
...					
Staff n					

A = Admin, U = User, G = Guest

----- จบ -----