ข้อกำหนดการเข้าถึงระบบสารสนเทศระยะไกล (Remote Access)

1. นโยบายการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายแบบ Remote Access

1.1 ไม่อนุญาตการเข้าถึงเครื่องแม่ข่ายผ่าน port80 ด้วยโปรแกรม Team viewer และ Logmein

1.2 สามารถเข้าถึงเครื่องแม่ข่ายแบบ Remote Access ช่องทางเดียวผ่านระบบ VPN ที่ Firewall ของสำนักหอสมุดที่มีการตรวจสอบตัวตนและสิทธิการเข้าถึงเครื่องแม่ข่ายแต่ละเครื่องตามนโยบายความปลอดภัยดังนี้

Server	Server Name	Allow Service	Admin/Root (External)	Staff (External)	Partners (External)
158.108.80.3	Agris-Office				
158.108.80.4	Agris-Web				
158.108.80.5	Millennium	SSH ,Telnet,http	✓	✓	✓
158.108.80.5	Millennium	FTP,SFTP	✓		*Migration
158.108.80.6	ILS Syswell	http,https			✓
158.108.80.8	Agris-	SFTP,SSH	✓		
158.108.80.10	Agris-				
158.108.80.12	e-Office	Remote Desktop	✓		
158.108.80.13	WEBLib	Remote Desktop	✓		
158.108.80.15	Language	Remote Desktop	✓		
158.108.80.16	Media	Remote Desktop	✓		
158.108.80.18	LMS Wiserf	http,https			✓
158.108.80.27	Agris-Web				
158.108.80.28	Resource	Remote Desktop	✓		
158.108.80.32	KOHA	SFTP,SSH	✓		
158.108.80.33	Paloalto	https	✓		✓
158.108.80.34	NetHAM	http	✓		
158.108.80.37	Time Stamp	Remote Desktop	✓		

158.108.80.38	CentOS	SFTP,SSH	✓		

2. นโยบายการเข้าถึงเครื่องแม่ข่ายแบบโดยตรง

2.1 สำหรับผู้ดูระบบ

2.1.1 ต้อง Scan Virus ก่อนนำอุปกรณ์จัดเก็บข้อมูลภายนอกมาเชื่อมต่อกับเครื่องแม่ข่าย

2.1.2 ที่เครื่องแม่ข่ายต้องตั้งค่า Online Auto Update Anti-virus และหมั่นตรวจสอบการทำงานอย่างสม่ำเสมอ

2.1.3 ตั้งค่าโปรแกรม Anti-virus ให้ Auto Scan External Drive

2.2 สำหรับบริษัท

2.2.1 ต้องได้รับการอนุญาต และอยู่ในการกำกับควบคุมจากผู้ดูแลระบบทุกครั้งตลอดการเชื่อมต่ออุปกรณ์เข้ากับเครื่องแม่ข่าย

3. กำหนดนโยบายการเปิดแชร์ไฟล์และโฟลเดอร์

3.1 กำหนดตัวบุคคลที่ชัดเจนที่มีสิทธิในการแชร์ไฟล์และโฟลเดอร์

3.2 กำหนดระดับชั้นของไฟล์ข้อมูลให้กับตัวบุคคลอย่างชัดเจน

3.4 กำหนดรหัสผ่านให้กับบุคคลที่มีสิทธิในการแชร์ไฟล์และโฟลเดอร์

4. กำหนดนโยบายการตั้งรหัสผ่านของเครื่องแม่ข่าย ,เว็บเซิร์ฟเวอร์ และฐานข้อมูลดังนี้

- ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ ๖ ตัวอักษร
- ควรใช้อักขระพิเศษประกอบ เช่น : ; < > เป็นต้น
- สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ ๖ เดือน
  ส่วนผู้ใช้งานที่มีสิทธิพิเศษ เช่น ผู้บริหารระบบ (system administrator) และผู้ใช้งานที่ติดมากับระบบ (default user) เป็นต้น ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ ๓ เดือน
- ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย
- ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “๑๒๓๔๕๖” เป็นต้น
- ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น
- ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม
- ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน ๕ ครั้ง
- ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที
- ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที