Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
The three hardening tools that should be implemented are : 1. Password policies 2. Multi factor authentication 3. Firewall maintenance Password policies Strengthens user authentication, reduces the risk of credential theft, prevents unauthorized access, and eliminates the risks tied to shared or weak passwords. MFA Adds an extra layer of security to user logins, ensuring that even if passwords are stolen, accounts stay protected. Firewall maintenance Controls and limits network traffic, blocks malicious or unnecessary access, and isolates sensitive systems to reduce exposure to external and internal threats.

Part 2: Explain your recommendations
1. Password policies are critical for implementation because employees share password, admins use default passwords which pose extreme risk for security. Long individual passwords with capital letters, small letters symbols, and numbers so the users and employees don't pose a threat to the security, and no longer share same passwords. A rule for regular change of passwords can be implemented for higher protection. 2. Multi factor Authentication to verify that only authenticated users can access protected data PI and PII, and will ensure 3. Firewall maintenance - Firewall should be updated to filter unwanted traffic from suspicious users. This maintenance should be done regularly so the system stay protected from potential old and new threats.