Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Based on the organizations vulnerabilities, the following hardening tools and methods are required to prevent further data breaches and attacks: 1. Password policies 2. Multifactor Authentication 3. Firewall maintenance

Part 2: Explain your recommendations
1. Password policies should be introduced due to the revealed vulnerability of employees sharing passwords and the administrator password for the database being left to the default making obtaining information extremely easy for a malicious actor. 2. Multifactor authentication will make malicious actors unable to breach security by adding an additional layer for them to be required to break through in order to carry out an attack. 3. Firewall maintenance is required because the network traffic needs to be filtered in order to detect if any packets coming in are malicious or corrupted to prevent any potential threats.