Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

I suggest following hardening methods to ensure these problems are fixed:

1. Problem: The organization’s employees' share passwords -
    - Solutions:
        - **Employees** must undergo **training** to refrain from sharing passwords
        - Password policy must require unique passwords which are longer and not repeated
        - Also create **security zones** to restrict access to systems
2. Problem: The admin password for the database is set to the default -
    - Solutions:
        - **Password policy** in place
        - The credentials to the admin password must be shared only with admins
        - **Passwords** must be changed frequently in case they are shared, changing them will reduce chances of unauthorised access later or from previous employees
        - Previous passwords must not be repeated
        - **Multifactor authentication** must be implemented especially for these roles which are high risk
3. Problem: The firewalls do not have rules in place to filter traffic coming in and out of the network.
    - Firewalls must be configured to **block unused ports**
    - Firewalls must **implement port filtering**
    - Firewalls must be configured in order to **block traffic** from suspicious & malicious sources
4. Problem: Multi Factor authentication (MFA) is not used.
    - **Multi Factor authentication** allows only authorised users to use certain resources
    - This involves adding a layer of authorisation apart from basic username password so that the identity of the user is confirmed before access is granted

Part 2: Explain your recommendations

1. Password Policy
    - Save passwords through hashing and salting
        - using methods to salt and hash passwords, rather than requiring overly complex passwords
        - Password policies are used to prevent attackers from easily guessing user passwords, either manually or through a brute force attack
    - Change password frequently
        - Since the employees share passwords it's essential that passwords are changed frequently
    - Stronger password usage
        - Training employees to use longer and mixed characters passwords or use password managers adds to password strength
    - Disable Repeating old passwords
        - If old passwords are shared they can be used to access systems by ex-employees or attackers who got unauthorised access to system
2. Firewall maintenance
    - Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.
    - Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks.
    - Block unused ports
        - Malicious actors might use dynamic ports for attacks or injecting code, these unused ports must be blocked in order to safeguard internal network from harmful attacks
    - Port filtering
        - A firewall function that blocks or allows certain port numbers to limit unwanted communication.
        - Port filtering is used to control network traffic and can prevent potential attackers from entering a private network.
3. Multi Factor authentication
    - A security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more.
    - This confirms the identity of the user and ensures that only authorised users have access to the resources
4. Security Zones
    - Network segmentation is a process of creating security zones in a way that allows specific users to access only part of network
    - So if a one segment is attacked then its impact gets limited to the zone in which attack took

place.