Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. **Password Policies:** Implement and enforce strong password policies across the organization, requiring employees to use complex passwords and prohibiting password sharing. 2. **Database Administration:** Change the default admin password for the database to a strong, unique password and restrict access to authorized personnel only. 3. **Firewall Configuration:** Configure the organization's firewalls to filter incoming and outgoing traffic based on predefined rules, blocking unauthorized access and potentially malicious traffic.

Part 2: Explain your recommendations
Enforcing strong password policies ensures that employees use secure passwords. By prohibiting password sharing, individual accountability is maintained, mitigating the risk of compromised credentials leading to unauthorized access. Changing the default admin password for the database eliminates the vulnerability posed by default settings, which are commonly known and targeted by attackers. Restricting access to authorized personnel ensures that only trusted individuals can modify sensitive database information. Configuring firewalls to filter traffic based on predefined rules helps control network access and prevent unauthorized connections. By blocking potentially malicious traffic, such as unauthorized attempts to access sensitive systems or services, the organization can reduce its attack surface and enhance overall security.