Security risk assessment report

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

Password policies;
Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack).make sure that every Employee and database password are following Password policies

Multi Factor authentication (MFA); 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.Use Google multifactor authentication recommended

Firewall maintenance; This can happen regularly. 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. Use Stateful or Cloud based firewall.It should be check every day or week for better protection and open only that ports which is useful to network which are to being used disable that ports

Part 2: Explain your recommendations

To set rules that employees can not share their passwords with anyone.The admin password for the database Should be Changed every week for better security and include Password Policy in that.Make sureThe firewalls have rules in place to filter traffic coming in and out of the network.Make sure Multi Factor authentication (MFA) is used.For extra protection