Part 1: Selected Hardening Tools and Methods

1. **Implement Multifactor Authentication (MFA)**
2. **Establish and maintain strict firewall rules**
3. **Enforce strong password policies**

Part 2: Explanation and Recommendations

1. Multifactor Authentication (MFA):
MFA adds an extra layer of verification by requiring users to provide two or more authentication factors (such as a password and a verification code). This measure significantly reduces the risk of unauthorized access, even if an attacker gains a user's password. MFA should be implemented across all employee and administrative accounts and enforced continuously.

Effectiveness: Prevents unauthorized logins and account takeovers by adding a verification step.
Implementation Frequency: Continuous — should remain permanently enabled and monitored.

---

2. Firewall Maintenance and Rule Configuration:
Firewalls serve as a critical defense layer by controlling traffic entering and leaving the network. Properly configured inbound and outbound rules can block malicious traffic, unauthorized connections, and data exfiltration attempts. Regular firewall audits ensure the rules remain relevant as systems and threats evolve.

Effectiveness: Filters unwanted or malicious network traffic, reducing the attack surface and preventing unauthorized access to internal systems.
Implementation Frequency: Initial configuration followed by reviews **weekly or monthly**, or after any major network changes.

---

3. Strong Password Policies:
Employees should follow strong password creation guidelines and avoid sharing credentials. Password policies should require a mix of letters, numbers, and symbols, and enforce password expiration and rotation schedules. The default admin password for the database must be changed immediately and stored securely.

Effectiveness: Prevents brute-force attacks and reduces the risks of weak or shared passwords.
Implementation Frequency: Policies should be enforced **continuously**, with periodic reviews and employee training sessions.

Summary

By enforcing MFA, regularly maintaining firewalls, and applying strict password policies, the organization can substantially reduce the risk of another data breach. Together, these measures address authentication, access control, and network boundary protection — the three primary points of failure in the original incident.