**Security Risk Assessment Report**

**1. Identification of Vulnerabilities and Recommended Network Hardening Tools**

**Vulnerability 1:** **Employees share passwords.**

* **Recommended Hardening Tool/Method:**
  + **Implement Strong Password Policies:** Establish strict password policies that enforce unique, strong passwords for all employees. Ensure that passwords are not shared and are changed regularly.
  + **Password Management Software:** Use password management tools that securely store and manage passwords, reducing the need for sharing passwords.

**Vulnerability 2:** **The admin password for the database is set to the default.**

* **Recommended Hardening Tool/Method:**
  + **Change Default Passwords:** Immediately change the admin password from its default to a complex and unique password. Default passwords are a common target for attackers.
  + **Password Rotation Policy:** Implement a policy that requires regular updates to critical system passwords, including the admin account.

**Vulnerability 3:** **Firewalls do not have rules in place to filter traffic coming in and out of the network.**

* **Recommended Hardening Tool/Method:**
  + **Firewall Configuration and Rule Implementation:** Configure firewalls to filter both inbound and outbound traffic. Establish rules that only allow necessary traffic and block all unauthorized access attempts.
  + **Regular Firewall Audits:** Conduct periodic audits and reviews of firewall configurations to ensure that rules are up to date and effective against new threats.

**Vulnerability 4:** **Multifactor Authentication (MFA) is not used.**

* **Recommended Hardening Tool/Method:**
  + **Implement Multifactor Authentication (MFA):** Enforce MFA for all critical systems and services, adding an extra layer of security by requiring a second form of authentication beyond just a password.

**2. Explanation of Effectiveness and Implementation Frequency**

**Tool/Method 1:** **Implement Strong Password Policies & Password Management Software**

* **Effectiveness:** Strong password policies help ensure that passwords are difficult for attackers to guess or crack. Password management software reduces the risk of password sharing and makes it easier for employees to manage complex passwords securely. This method significantly reduces the risk of unauthorized access due to weak or shared passwords.
* **Implementation Frequency:** Password policies should be enforced continuously, with periodic training for employees. Password management tools should be used daily, and password policies should require password changes every 60-90 days.

**Tool/Method 2:** **Change Default Passwords & Implement a Password Rotation Policy**

* **Effectiveness:** Changing default passwords immediately removes a common entry point for attackers. Regularly rotating passwords ensures that even if a password is compromised, it won't be valid for long, reducing the window of opportunity for attackers.
* **Implementation Frequency:** Default passwords should be changed immediately upon system setup. Passwords should be rotated at least every 90 days for critical accounts, with reminders set up to enforce this policy.

**Tool/Method 3:** **Firewall Configuration and Rule Implementation**

* **Effectiveness:** Properly configured firewalls act as a barrier between the internal network and external threats, blocking unauthorized access while allowing legitimate traffic. Regular audits ensure that firewall rules adapt to new threats and changes in network configuration.
* **Implementation Frequency:** Firewalls should be configured at setup and reviewed every 6 months or whenever there is a significant change in network infrastructure.

**Tool/Method 4:** **Implement Multifactor Authentication (MFA)**

* **Effectiveness:** MFA adds an additional layer of security by requiring a second factor of authentication, such as a code sent to a mobile device, reducing the risk of account compromise even if passwords are stolen.
* **Implementation Frequency:** MFA should be implemented as soon as possible and be mandatory for all critical accounts. The second factor should be changed or updated regularly, depending on the method used (e.g., mobile apps, hardware tokens).