# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| The data breach left user information compromised, not just for employees but users of the site as well. External user information was compromised. To insure this does not happen in the future. I would recommend the following:  MFA and Password Policies  Port Filtering  Encryption using the latest security standards. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| The recommendations are based on the following security issues:   1. The organization’s employees' share passwords. 2. The admin password for the database is set to the default. 3. The firewalls do not have rules in place to filter traffic coming in and out of the network. 4. Multifactor authentication (MFA) is not used.   All employees are to use Multi Factor authentication (MFA) for their workstations, alongside a new password policy ensuring more complex passwords prior to sign on. Users on the site will also be strongly encouraged to set up MFA of their own and they will be required to change their password on their next sign on. This falls under review on the principles of Password Policies and MFA. Although these can be separate policies within their own right, for the purposes of this Risk Assessment they will be treated within the same umbrella of scope. With regards to the admin password for the database, I would recommend the same as the above. Further, I would recommend a hardening of the admin password for the database with a stipulation that the password policy, whereby a change request for the password would need to be signed off by the Senior Manager of staff for the IT department, before a change can take place. This will adhere to the principle of security in depth.  A firewall reconfiguration is required to allow traffic or block traffic that is unwanted or perceived as dangerous. We can integrate the firewall rules with the credentials on the database to allow users and employees access while blocking network traffic that is not recognized by the database. This process can be automated to insure new hires are seamlessly given the correct credentials while business leavers and users that remove their accounts have their information wiped from the database in a legally compliant and effective manner.  As a rule we need to encrypt all traffic on the site and in the office. We should make sure that the website is connecting through TCP/IP port 443 to allow for HTTPS TLS connections and enforce a VPN policy for off-site workers to ensure that the data they are transmitting is secure.  The above recommendations will not only insure that a breach of this nature does not happen again, but it will also insure the safe and compliant handling of sensitive data within the company. |