# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| Network access privileges, password policies, firewall maintenance. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| The main issues are weak passwords, large attack surface due to employees sharing information, and a lack of a working firewall. Changing the password from the default, potentially using salt and hash passwords, will immediately make it harder for malicious actors to gain access to the network. Network access privileges, such as segmentation, and better policies about who employees should share passwords with will reduce risk. This also helps narrow down the accountability for a breach, and isolate the breach. A working firewall is very important because it serves as the main block between outgoing and ingoing traffic. Without it, a LAN is completely exposed to the wide web. Implementing even a basic firewall will neutralize a bulk of simple attacks (such as DoS attacks). |