



Prevent Cyber Security Incidents by Following Best Password Practices

Passwords are one of the most commonly used security mechanisms to prevent unauthorized access to systems and sensitive information. However, if people select weak passwords, the risk of an incident occurring rises.

Please consider the following practices to create and use passwords:



Use passwords that **are hard to guess**. Avoid using words like: your employee ID, the name of the company, name of your favorite sport team, etc.



If your current **passwords are easy to guess** (e.g., Company123, Company2016, password, etc.) or default passwords (letmein, admin, etc.), please **change them**.



Create passwords of at **least eight characters**. Use a combination of **numbers, capital letters and lowercase letters**. Avoid words that can be found in the dictionary.



Do not store your list of passwords on your computer in plain text, nor on a post-it or piece of paper that are easily accessible to other people.



Change your passwords frequently, avoid using the same password for different applications, and Do not share your password with anyone

The following list shows some of the worst passwords, please avoid using them:

- | | | |
|------------|-----------------------|--------------------------|
| • 12345678 | • Login | • Car brand name + model |
| • Password | • Letmein | • Sport team name |
| • abcd1234 | • 1qaz2wsx | • User ID |
| • qwerty | • Admin | • Employee number |
| • 11111111 | • Month name + year | • Football |
| • Passw0rd | • Company Name + year | • Computer Brand + year |

Enterprise Information Security Management

security.culture@cemex.com