# Goldman Sachs Virtual Internship

200 West Street

New York City, NY 10282

[inbox.kpatel@gmail.com](mailto:inbox.kpatel@gmail.com)

June 12, 2022

To whom it may concern,

After analyzing your password systems, I concluded the organization uses an outdated password hashing algorithm known as M05. In the possible event of a password database leaking, M05 offers very little protection. M05 is not industry standard and shows that the current password policy at your organization is not aligned with the industry best practices.

The current password policy at your organization consists of:

* The minimum length for a password is set to 6.
* There is no specific requirement for password creation. Users can use any combination of words and letters to create a password.

To meet industry standards and maintain best practices, Secure Hash Algorithm (SHA) and Message Digest (MD5) cryptographic hash functions should be used alongside several new requirements in your password policy. My recommendations are:

* Avoid common words and character combinations in your password
* Longer passwords are better. 8 characters is a starting point
* Don't reuse your passwords
* Include special characters, Capital and Small letters, and numbers in your password.
* Do not let users include their username, actual name, date of birth and other personal information while creating a password.
* Train your users to follow all these policies.

Best regards,

Karan Patel

Computer Science Student

**Security Algorithms used:**

experthead:e10adc3949ba59abbe56e057f20f883e – MD5 interestec:25f9e794323b453885f5181f1b624d0b – MD5 ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 –MD5

reallychel:5f4dcc3b5aa765d61d8327deb882cf99 –MD5 simmson56:96e79218965eb72c92a549dd5a330112 – MD5 bookma:25d55ad283aa400af464c76d713c07ad – MD5 popularkiya7:e99a18c428cb38d5f260853678922e03 – MD5 eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 – MD5 heroanhart:7c6a180b36896a0a8c02787eeafb0e4c – MD5 edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 – MD5 liveltekah:3f230640b78d7e71ac5514e57935eb69 – MD5 blikimore:917eb5e9d6d6bca820922a0c6f7cc28b – MD5 johnwick007:f6a0cb102c62879d397b12b62c092c06 – MD5 flamesbria2001:9b3b269ad0a208090309f091b3aba9db – MD5 oranolio:16ced47d3fc931483e24933665cded6d - MD5

spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e - MD5

moodie:8d763385e0476ae208f21bc63956f748 - MD5

nabox:defebde7b6ab6f24d5824682a16c3ae4 - MD5

bandalls:bdda5f03128bcbdfa78d8934529048cf - MD5

**Cracked Passwords:**

experthead:e10adc3949ba59abbe56e057f20f883e - 123456 interestec:25f9e794323b453885f5181f1b624d0b - 123456789 ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 - qwerty reallychel:5f4dcc3b5aa765d61d8327deb882cf99 - password simmson56:96e79218965eb72c92a549dd5a330112 - 111111 bookma:25d55ad283aa400af464c76d713c07ad - 12345678 popularkiya7:e99a18c428cb38d5f260853678922e03 - abc123 eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 - 1234567 heroanhart:7c6a180b36896a0a8c02787eeafb0e4c - password1 edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 - password! liveltekah:3f230640b78d7e71ac5514e57935eb69 - qazxsw blikimore:917eb5e9d6d6bca820922a0c6f7cc28b - Pa$$word1 johnwick007:f6a0cb102c62879d397b12b62c092c06 - bluered