



ALZEWAYED GROUP
ALZEWAYED GROUP

Password **P**olices
Don't Compromise



Dear Alzewayed Group employees,

Personal and financial information is sent across the internet with little to no hesitation in our digital world. We use phones and tablets on open internet connections to access apps and websites containing banking information, personal contact information and other information that should typically be secure and private.

In this open digital world, the password became our identity and choosing the right password which ruled by the best practiced policies will insure your safety and the company information security.

For this reason, you will found in this guide Alzewayed Group password policies which will help you keeping your identity safe and secure.



Index

Company Password Policy.....	1
10 tips to create strong password.....	2-4
Changing Gmail password.....	5-6
Changing other email password “@alzewayed.com.sa, @sist.com.sa, @mccl.com.sa”	7
Changing SIS system password.....	8
Changing Domain & Microsoft Dynamics password....	9
Contact Us.....	10



Company Password Policy

Domain Users Password Policy

- Password have to be change after the 1st login.
- Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.
- Passwords must be at least eight characters in length or the number of characters specified in the **Minimum password length** policy setting.
- Passwords must contain characters from at least three of the following four categories:
 - English uppercase alphabet characters (A–Z)
 - English lowercase alphabet characters (a–z)
 - Base 10 digits (0–9)
 - Non-alphanumeric characters (for example ~!@#\$%^&* _ - +=`\'\"{}[]:;\"'<>.,?/).
- The password has to be changed every 90 days.

Gmail Account Password Policy

Google Account passwords must be at least 8 characters long. They can include:

- Uppercase and lowercase letters. Passwords are case-sensitive, so "G" is different from "g."
- Numbers
- These symbols: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ { | } ~
- Spaces: You can't use a space at the beginning or end of your password, but spaces inside the password are fine.

Keep in mind, you won't be able to reuse a password from the past year. Gmail have also blocked some passwords that are easy to guess, like "12345678" or single character password.



10 Tips to Create Strong Password

1. Create a Strong Password

Simply creating a strong password is the easiest way to halt hackers from getting inside. Password strength can be measured by the 8 + 4 rule. This means the password has at least 8 characters and at least one upper case, one lower case, one number and one special character.

Here's an example of a password following the 8 + 4 rule:

l3M0nT@rt

The more random, the better. There are a lot of users that attempt to use simple patterns to create a "random" password, but it only appears random. A password like this is a welcome mat:

ABC123abc

2. No Personal Information

It's surprising how many users incorporate personal information into their password to help them remember. Security specialists examined the LinkedIn passwords that were hacked and a surprising number simply had the user's first name with their birth year. For example:

mike1982

3. Create Unique Passwords for Each Account

This is a particularly dangerous scenario. If your users use the same password for all of their accounts, the hacker can then use them to get into personal email, work email, network logins, Facebook and even bank accounts. Research polls estimate that about 25% of people use a single password for all of their accounts.



4. Never Write Them Down

Using a separate password for each account can get extremely tricky, because the average online user has 26 different accounts that require passwords.

People 35 years old and younger average up to 40 accounts.

Despite the difficulty in remembering all of these passwords, it is essential that your users never write them down or store them on their computer.

5. Change Passwords Frequently

Experts suggest that the longest your users should keep any password is six months or less. The ideal timeframe is closer to three months, particularly for accounts that have critical functionality (such as bank accounts).

6. Beef Up Computer Security

If the end user's computer has spyware or viruses, it doesn't really matter how diligently their passwords are maintained. Every computer on the network, including home computers that are used to access the network remotely, must have an enterprise-level security program.

7. Use a Password Checker

There are reputable companies that offer free password checking that are encrypted for extra protection. Microsoft offers a [password checker](#) online. Apple also has their Password Assistant embedded into their operating system.

8. Never Share

Sharing a password, particularly over a digital forum (chat, email, private message boards), is a big no-no. Network user should understand that emails (even internal emails) should be treated like a postcard.



The only acceptable time to share a password is with the internal help desk. Even then, the password should be immediately changed following the conclusion of the assistance.

9. 'Remember Password' Setting

A lot of internet browsers offer the capability to remember passwords for the ease of their users. This is a major security risk, particularly for laptops. If the laptop is stolen and the initial OS login can be circumvented, then all of the users' accounts are open for intrusion. These settings can be turned off in Chrome, Firefox and IE quite easily.

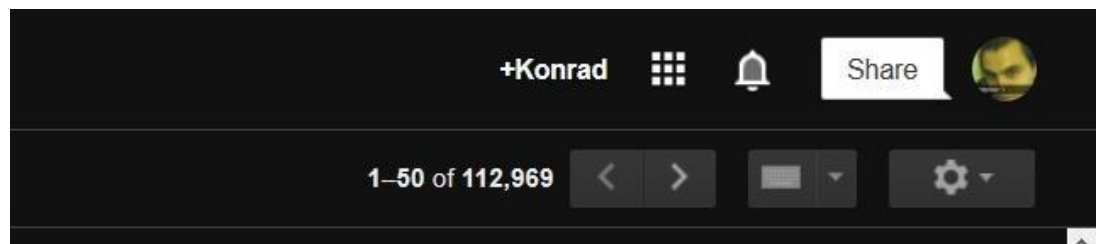
10. Protect Everything

Almost every device you have can connect, communicate, and browse the internet or the network. That's why it is essential that the same data governance and security protocols that are implemented for PCs are also enforced for laptops, tablets and smart phones.

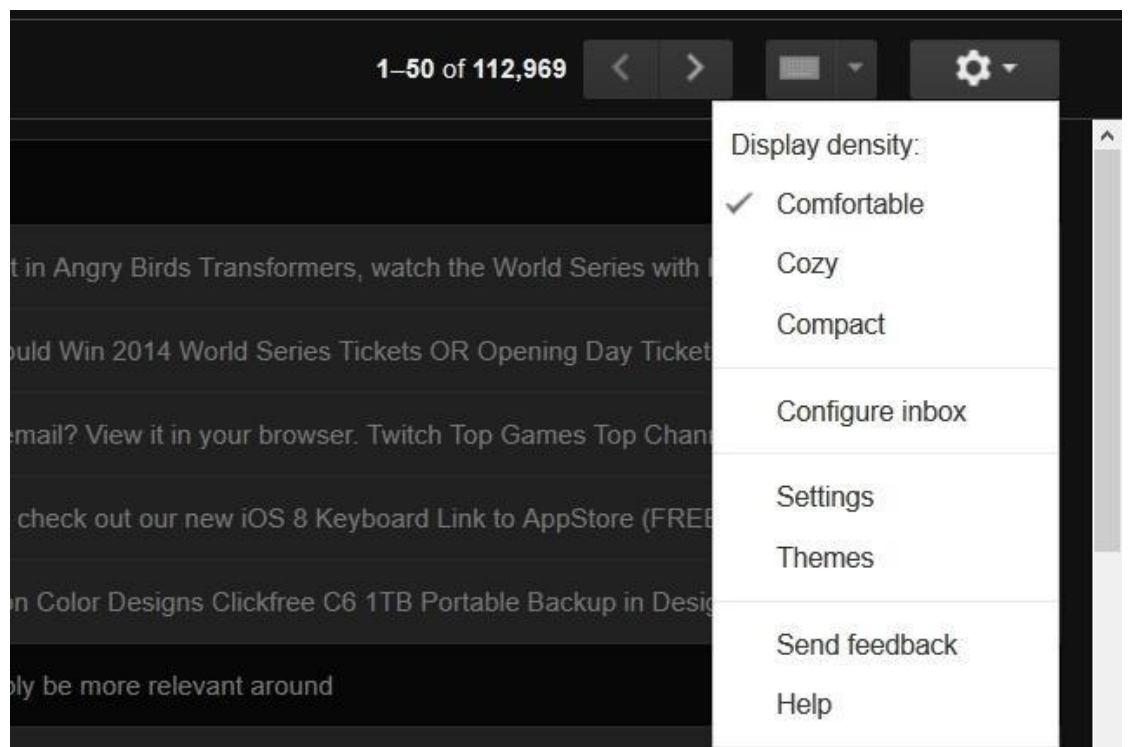


Changing Gmail password

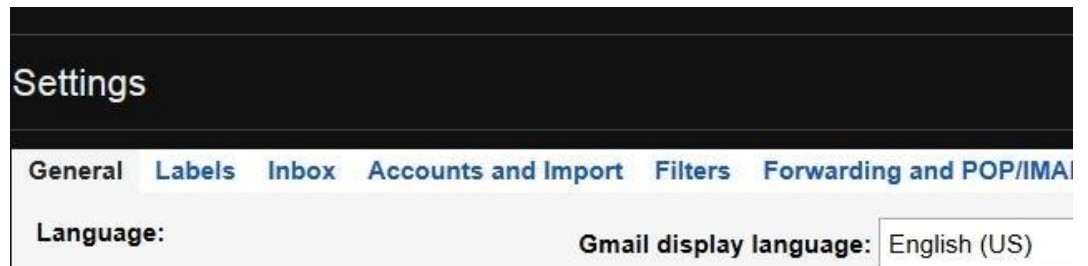
Step 1. Log into your Gmail account, and click the gear icon in the upper right-hand corner.



Step 2. Click “Settings.”

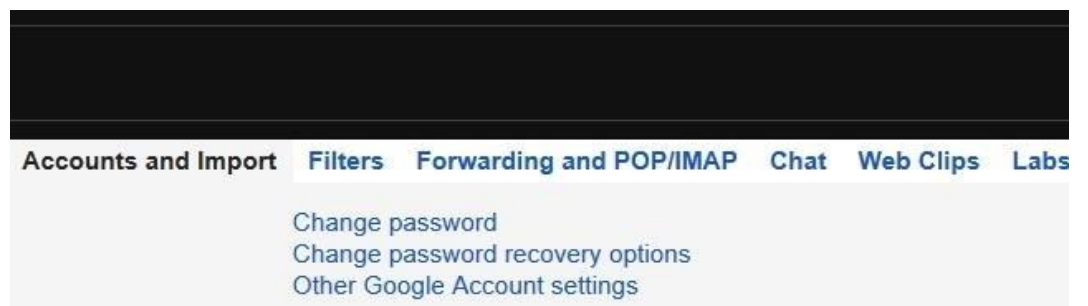


Step 3. Click “Accounts and Import” at the top.



The screenshot shows the Gmail 'Settings' page with the 'Accounts and Import' tab selected. The 'Language' section is visible, showing 'Gmail display language' set to 'English (US)'.

Step 4. Click “Change password.”



The screenshot shows the 'Accounts and Import' settings page. Under the 'Accounts and Import' tab, the 'Change password' link is highlighted.

Step 5. Here, you’ll be required to enter your current password, along with your new password twice. Note that you can’t reuse an old password once you change it. Plus, any Gmail password you use must consist of eight characters. Once you satisfy these requirements, just click the blue “Change Password” button, and you’ll be good to go!



The screenshot shows the 'Change Password' form. It includes fields for 'Current password', 'New password', and 'Confirm new password'. There is a link for 'Don't know your password?' and two buttons at the bottom: 'Change Password' and 'Cancel'.



Changing other email password.


“@alzewayed.com.sa, @sist.com.sa, @mccl.com.sa”

Step 1. Login to Webmail.

Step 2. Click the Change Password button.



Step 3. In the box to the right of Password, type the new password for the email address.

 **Change Mail Account Settings**

The system is changing the password for ... example@example.com

New Password:

Confirm Password:

Strength (Why?): Very Weak (0/100) Password Generator

Change Password

← Go Back

Step 4. In the box to the right of Password (again) type the new password again.

Step 5. Click Change Password button.

Step 6. Your screen should refresh and you should receive a confirmation page. Congratulations! You've successfully changed your email account's password.



Changing SIS system password

Step 1. Login to www.ereg.gc.edu.sa with your username and password.

Step 2. Click security then Change Password button.



Step 3. In the box to the right of Old Password, type your old password.

Step 4. Fill your new password field and confirm it.

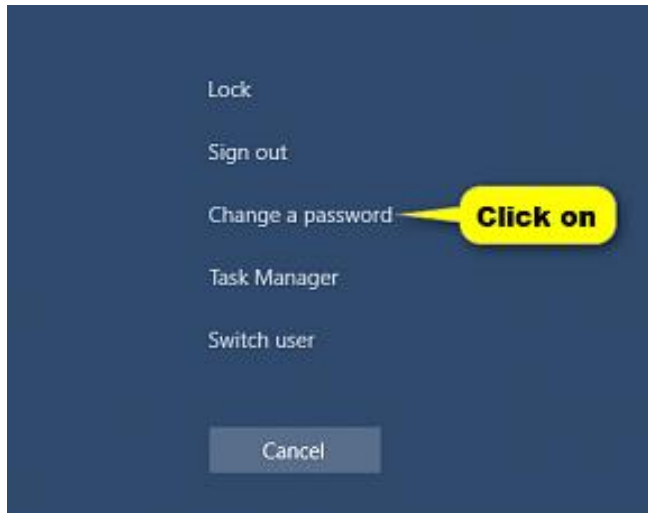
A screenshot of the 'change password' dialog box. It contains four input fields: 'Old Password*', 'New Password*', 'Confirm Password*', and 'Last update'. The 'Last update' field is pre-filled with '7-08-1436'. There are 'Save' and 'Cancel' buttons at the bottom.

Step 3. Push the save button and your password will be change.

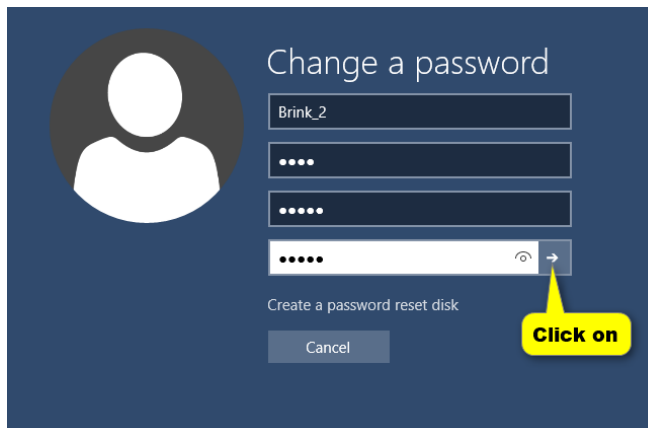


Changing Domain Password.

Step 1. While signed in to your local account, press the CTRL+ALT+DELETE keys to open the secure screen and then tap or click Change a password.



Step 2. Type in your current old password, type in a new password, and press Enter or click/tap on the arrow.



For more information or questions

kindly contact us at

it@alzewayed.com.sa

web: www.it.alzewayed.com.sa



Information Technology
Department

ALZEWAYED GROUP **الزعيدي**

مجموعة شركات