1. You have started working for a medium sized firm of around 25 users. This firm specializes in selling valuable jewelry.

As the new IT Administrator, you find out the following:
1. Password length is generally 6 characters which is not very good
2. Passwords never change. That is not good either
3. There is no maximum age for passwords
4. No Time of day restrictions

You will need to modify the password policy. Due to the size of organization, the IT manager (that is you), does not have the power to make big changes and certainly cannot enforce it. What would you recommend in the real-world environment as a best practice?

Passwords

Password length
- minimum password length of at least 14 characters, mix of characters;
- strong passphrases encouraged, examples include all four character types:
  - uppercase letters;
  - lowercase letters;
  - one or more numbers;
  - and one or more special characters;
  - examples: IL0veSecurity+, IL0veThi$B00k, and IWi11P@$$;

  - nonsensical string not encouraged: 4*eiRS@<];
  - user's name, words in dictionary (for any language), or common key combinations not encouraged;
  - writing down passwords not encouraged;

Password change
- Change password every 45 or 90 days;
- Password expires when users are no longer able to log on because prompted to first change their password;
- Temporary password given for password reset and expires upon first use;
- Change password immediately after logging on when temporary password expires;

Maximum age for passwords
- Password history system to remember past passwords and prevent users from reusing;
- Password expiration requiring new password that has not been entered;
- Password policy settings to prevent users from using last 24 passwords entered;
- Password can possibly be reused if 24 new passwords have been entered;

Time of day restrictions
- User can log on to the network during timeframe and not outside restricted time;
- If user tries to log on outside of restricted time, the system will deny access;
- Overtime does not log the user out of the system although the user is not logged on during restricted time;
- System will prevent from creating any new network connections, even if logged on, if outside of restricted time;

- CompTIA Security+ Get Certified Get Ahead

2. Briefly explain the difference between “Something You Are” and “Something You Have” methods of authentication.

Something You Are
- The something you are authentication factor uses biometrics for authentication. Biometric methods are the strongest form of authentication because they are the most difficult for an attacker to falsify. In comparison, passwords are the weakest form of authentication.
- Something you are, using biometrics, such as fingerprints or retina scans
- somewhere you are — An authentication factor indicating location, often using geolocation technologies.

- Something You Have
- The something you have authentication factor refers to something you can physically hold;
- ...common items in this factor, including smart cards, Common Access Cards, and hardware tokens.
- Something you have, such as a personal identity verification;
- something you have — An authentication factor using something physical;

- CompTIA Security+ Get Certified Get Ahead