ISO/IEC 27001:2013 Information security management systems
-User responsibilities-

Security category – 9.3. User responsibilities

Control – 9.3.1. Use of secret authentication information
The users are to be required to follow the organization’s procedures for the use of secret authentication information.

***Users need to be aware of the fact that they can be held accountable for someone else using their passwords*.**

ISO/IEC 27001:2013 Information security management systems
-User responsibilities-

ISO/IEC 27002 guidelines for users choosing and managing passwords:

- users should be advised to keep secret passwords confidential;
- avoid keeping a record of passwords (unless there is a password vault app);
- if possible compromise - change the password;
- advice users not to use the same password for both business and non-business purposes
- select quality passwords
    - sufficient length but be easy to remember;
    - not based on things easy to guess (name, birthdate),
    - not vulnerable to dictionary attacks.

Single Sign On – convenience (don't have to remember multiple passwords)
- security risk (in case it is compromised)