Access Management Rules

1. Unique user IDs **MUST** be used to access Klarna's systems.
2. The user IDs **MUST** be employees' corporate email addresses.
3. Use of group IDs **MUST NOT** be permitted.
4. The level of access granted **MUST** be appropriate to the business need.
5. A formal record of all persons having access to the system **MUST** be maintained.
6. User access to Klarna's systems **MUST** be revoked if an employee leaves the company or changes job responsibilities.
7. User IDs that have been in use by one person **MUST** not be issued to other users.
8. Passwords **MUST** be unique to the individual Klarna account and not reused elsewhere.
9. Passwords **MUST** be changed regularly (at least every 12 months).
10. Passwords **MUST** have a minimum length of 14 characters.
11. Password **MUST** contain characters from at least three of the following categories:
    a. Uppercase English letters (A-Z)
    b. Lowercase English letters (a-z)
    c. Digits (0-9)
    d. Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
12. Users **SHOULD** enable 2FA on all accounts.
13. It is your responsibility to protect your account credentials and inform Klarna about any unauthorized use of your account.
14. Passwords **SHOULD** be generated and managed with a Password Manager.