密码存储原则

在密码存储安全上，防止数据管理员批量泄漏用户口令，因此在密码存储上可定义下级级别。

级别	描述	风险
低	密码为明文	泄漏用户信息就泄漏密码
中	密码为密文，但同一密码密文相同	通过比对密文，还是能推导出密码
高	密码加偏移量的密文	保正同一密码，密文都不一样

密码安全原则

共享密码：设定共享密码时，请选择一个没有在其他任何地方使用的密码。如果你在另一个服务也使用相同的密码，攻击者可以同时获得两个云服务的访问。

密码有效时间：假定攻击者已经破解了密码，并可以访问云服务，那么每 90 天修改一次密码就非常关键。这种做法有助于防止攻击者进一步取得认证并窃取更多的敏感信息。

密码最短长度：密码长度应至少 8 位，虽然我们通常建议更长的密码。为了安全起见，造一个句子来作为你的密码。

密码强度：密码应该同时使用小写和大写字母，数字和特殊字符。这确保攻击者在暴力破解密码时必须通过更多数量的组合才能成功。

密码历史：保存并使用密码的历史版本，这让系统能够比较当前密码与历史密码并确定有些密码是否会过于相似。如果过于相似的话，应该拒绝本次密码更改

基于上列原则，因此在用户重置密码时，我们应按下列规则的告知客户密码强度。

安全级别	强度描述
警告	少于 8 位
警告	常用弱密码
低	大于等于 8 位
中低	含有数字或者字母
中	含有小写和大写字母

安全级别	强度描述
中高	含有数字和小写和大写字母
高	含有小写和大写字母，数字和特殊字符

同时在安全性更高的应用上，我们需要启用，**密码有效时间**和**密码历史**效验，同时明确密码强度在在中高以上，密码重置才可通过，并排除弱密码。

国内弱密码

> 国内网民常用的 25 个弱密码包括：000000、111111、11111111、112233、123123、123321、123456、12345678、654321、666666、888888、abcdef、abcabc、abc123、a1b2c3、aaa111、123qwe、qwerty、qweasd、admin、password、p@ssword、passwd、iloveyou、5201314、asdfghjkl、66666666、88888888

国外弱密码

> 国外网民常用的 25 个弱密码包括：password、123456、12345678、qwerty、abc123、monkey、1234567、letmein、trustno1、dragon、baseball、111111、iloveyou、master、sunshine、ashley、bailey、passw0rd、shadow、123123、654321、superman、qazwsx、michael、football、asdfghjkl