NIST Password Guidelines (NIST SP 800-63)

	Aspect	NIST Recommendation
1	Character length	64 characters minimum (8 is absolute min to be considered secure)
2	Case-sensitive	Yes
3	Allowed character set	Unicode
4	Require complexity rules	No
5	Force password change periodically	Only upon evidence of compromise
6	Passwords stored as hashes	Yes
7	Use of a PBKDF2-class one way hash function (RFC 8018)	Yes, minimum of 10K iterations
8	Use of password salt prior to hashing (NIST SP 800-90)	Yes, minimum of 32 bits in length and randomly generated
9	Both salt and password hash stored securely	Yes
10	Additional hash iteration with Pepper (secret salt)	Yes
11	Pepper is stored separately from password hash and salt	Yes
12	Allows paste functionality into password field	Yes
13	Show password feature	Yes
14	Contains repetitive or sequential characters	No
15	Contains dictionary words	No
16	Allows password found in published breaches	No
17	Allows username in password	No
18	Allows context in password (service name, service acronym, etc.)	No
19	Password strength meter	Yes
20	Failed attempt limit	100 consecutive failed attempts
21	Failed attempt lock out time	30 seconds to 1 hour
22	Bot detection after failed attempt	CAPTCHA
23	Whitelist IP address from previous successful attempts	Yes
24	Adaptive authentication detection (geolocation, request patterns, etc.)	Yes
25	MFA for account recovery	Yes

References

Document	Link
NIST SP 800-63B Version 3	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
Approved random bit generator	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
RFC 8018 (January 2017)	https://www.rfc-editor.org/rfc/rfc8018.html
FIPS 140-2 (Secure Crypto)	https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf
SP 800-131A Rev. 2 (Key Length)	https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final