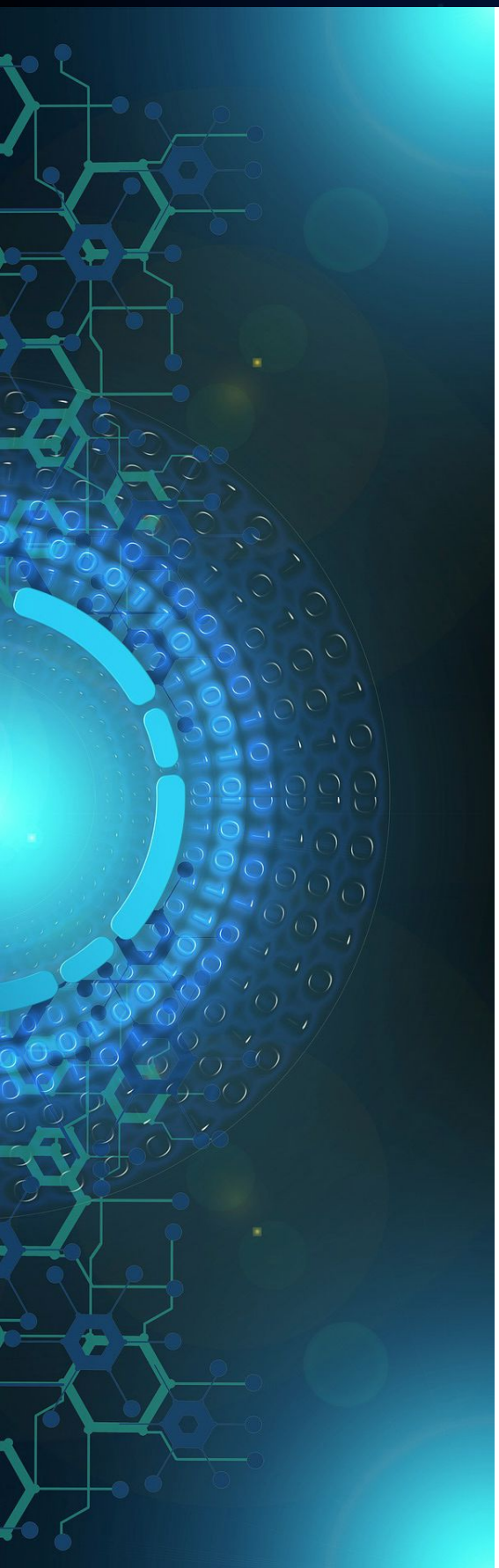

PASSWORD SECURITY COMPLIANCE

Reduce risk and ensure compliance by managing password strength and policy.

Overview

Passwords are a critical component of security. Passwords serve to protect user accounts; however, weak passwords may violate compliance standards, be reversed engineered back to plaintext and sold on the dark web, or result in a costly data breach if compromised. A periodic review of password rules is a vital component of your compliance and security strategies.

Purpose

The purpose of this security brief is to inform organizations of key password requirements and initiate internal compliance conversations. Use this security brief as a tool to enforce or strengthen your existing password policy.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

Verizon BDIR 2017

According to Verizon's 2017 Data Breach Investigations Report, 81% of hacking-related breaches leveraged either stolen and/or weak passwords. Financial, healthcare and public sector organizations accounted for over half of those breaches.

Password strength is an important security concern. With over four billion credentials stolen last year and data breaches averaging $3.62M in direct costs per incident, companies must be prepared for the security risks they face.

While all applications should apply password constraints to discourage easy to guess passwords, many organizations are required to do so by law. It is necessary to have stringent password constraints in place in order to comply with industry regulations.

Compliance is about fostering a culture that values user data and integrity and that culture starts at the top. A CEO must begin by looking at governance: the policies, controls and rules that represent their organization. This at-a-glance overview outlines the strict requirements of industry specific password compliance and will help you initiate critical conversations with your engineering, security and governance teams.

FDA

HIPAA

PCI

AICPA Service Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports

NIST

FDA (U.S. Food and Drug Administration)

FDA regulates food, drugs, biologics, medical devices, electronic products (that give off radiation), cosmetics, veterinary products, and tobacco products.

- [ ] At least 8, but no more than 32 characters
- [ ] At least one uppercase letter
- [ ] At least one lowercase letter
- [ ] At least one special character
- [ ] At least one number
- [ ] Passwords must be changed every 90 days

HIPAA (Health Insurance Portability and Accountability Act)

Any organization that deals with protected health information (PHI) must ensure HIPAA compliance.

- [ ] At least 6, preferably 8, characters in length
- [ ] Combination of uppercase and lowercase letters, mixed with numbers and symbols
- [ ] Password should be changed every 45 to 90 days
- [ ] Cannot be the same as any of the user's last 12 passwords

PCI DSS (Payment Card Industry Data Security Standard)

Any organization that deals with payment card data must be PCI compliant – whether payment card processing is the company's primary function or not.

- [ ] At least 7 characters
- [ ] Have a mix of both letters and numbers
- [ ] Passwords must be changed every 90 days
- [ ] Cannot be the same as any of the user's last four passwords

SOC 2 (Service Organization Control)

Established by AICPA, SOC 2 applies to all companies using the cloud to store customers' information.

- [ ] At least 8 characters in length
- [ ] Lower and uppercase letters
- [ ] One number
- [ ] One symbol

NIST (National Institute for Standards and Technology)

NIST produces guidelines to help federal agencies meet the requirements of the FISMA, however other organizations reference NIST for strong security standards.

- [ ] Minimum of 8 characters
- [ ] Allow a maximum length of at least 64 characters
- [ ] No more mandatory password changes
- [ ] No special characters requirements

The NIST guidelines were published in June 2017. NIST sets the precedence and these standards often trickle down to other regulations, such as HIPAA and SOC. It is likely there will be a shift in favor of password length and user friendliness.

"Passwords that are too short yield to brute force attacks as well as to dictionary attacks using words and commonly chosen passwords."

NIST Digital Identity Guidelines

Conclusion

Password security is a vital part of compliance. Maintaining security and compliance allows organizations to protect user data and maintain customer trust.

Rules and regulations surrounding compliance certifications are constantly changing and meeting the specific standards can be difficult. Selecting the right technology partner, with built-in capabilities, can help companies strengthen password security and policy easily to keep customer information secure, meet compliance standards and keep business thriving.

About FusionAuth

FusionAuth was designed and built by security and identity experts with over 50 combined years experience developing software for Fortune 500 companies. It installs in minutes and delivers Customer Identity and Access Management including login, registration, SSO, MFA, emails, localization, reporting and powerful user management features.

FusionAuth has been battle-tested in high-volume industries from finance to gaming and deployed on servers around the globe. For more information, visit fusionauth.io.