OLOID

PASSWORDLESS AUTHENTICATION IMPLEMENTATION CHECKLIST

01. Risk Assessment

- Evaluate security needs and identify suitable authentication methods.
- Assess threat landscape and understand potential vulnerabilities.
- Determine authentication requirements for different user groups and systems.

02. Industry

- Choose appropriate authentication factors (biometrics, tokens, mobile devices, or FIDO2).
- Select compatible hardware (e.g., fingerprint scanners, security key readers) and software platforms (e.g., identity management systems, authentication servers).
- Consider integration with existing systems and infrastructure.

03. User Education

- Communicate the benefits of passwordless authentication.
- Provide clear instructions on how to use the new authentication methods.
- Address user concerns about data privacy and security.

04. Pilot Testing

- Select a representative group of users to test the new authentication methods.
- Monitor performance, track user experience, and identify technical issues.
- Gather feedback and refine implementation based on pilot results.

05. Full Deployment

- Develop a phased approach for rolling out passwordless authentication across the organization.
- Provide support to users during the transition.
- Monitor adoption rates and user acceptance of the new authentication methods.

06. Ongoing Management

- Regularly assess the effectiveness of the passwordless authentication system.
- Stay updated on emerging security threats and implement countermeasures.
- Update authentication methods as needed and consider incorporating new technologies.

07. Additional Considerations

- Implement multi-factor authentication (MFA) for enhanced security.
- Prioritize user experience and avoid creating unnecessary friction during login
- .Ensure accessibility for users with disabilities.
- Adhere to relevant industry regulations and standards.