SECURITY BRIEF

Business Information Security

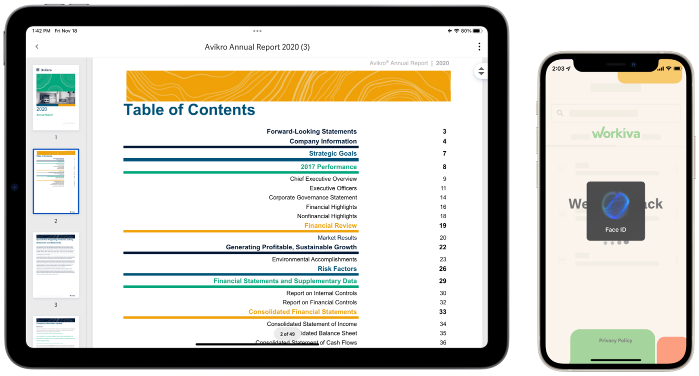
Mobile Application Security Brief

Workiva Mobile Application Security

We realize that the data stored within our platform is confidential and highly sensitive. We also understand that device-based access to data is often required. Our mobile platform is an extension of the Workiva platform, which includes numerous physical, logical, and operational security measures. Our mobile applications are designed and developed with careful consideration given to customer data security, reliability, and integrity. Policies and procedures are in place to ensure security at every phase of design, deployment, and ongoing operations.

Mobile users will be able to experience the Workiva platform without discounting on security, as the data continued to be encrypted in transit and at rest within the Workiva platform and no data is stored on end user mobile devices. Mobile application leverage existing security controls from Workiva platform including privacy.

FIGURE 1: Wdesk Mobile running on a tablet



1:42 PM   Fri Nov 18

Avikro Annual Report 2020 (3)

Avikro® Annual Report | 2020

Table of Contents

Forward-Looking Statements	3
Company Information	4
Strategic Goals	7
2017 Performance	8
Chief Executive Overview	9
Executive Officers	11
Corporate Governance Statement	14
Financial Highlights	16
Nonfinancial Highlights	18
Financial Review	19
Market Results	20
Generating Profitable, Sustainable Growth	22
Environmental Accomplishments	23
Risk Factors	26
Financial Statements and Supplementary Data	29
Report on Internal Controls	30
Report on Financial Controls	32
Consolidated Financial Statements	33
Consolidated Statement of Income	34
idated Balance Sheet	35
Consolidated Statement of Cash Flows	36

2 of 49

The Workiva Mobile application for iOS and Android provides device based access to business information stored within the Workiva platform. Mobile application is by design has limited features and allowing only authorised users to perform limited actions such as viewing a document.

This brief describes the implementation we have in place to ensure the utmost in data security and privacy for mobile devices.

The Workiva Mobile application includes:

- **Encryption** - Protecting our customer’s data is at the core of what Workiva does. Workiva mobile app doesn't store any data locally on mobile devices thus reducing overall risk. Network communication is encrypted and transferred via TLS 1.2+. Secure transmission is enforced for all access.

- **Authentication Mechanisms**—Leverage your existing Workiva platform authentication controls with the mobile apps. Multi-factor authentication, SSO with SAML 2.0 or set your own password composition requirements via Workiva platform settings. Users can opt-in to use biometric recognition such as Face ID, Touch ID on their devices, note that Workiva does not have access to any biometric data.

- **Timeout Lock**—A timeout limits the idle time of the app, locking it with passcode authentication if exceeded.