Optician Management Software

The Gables Church Lane
Hungarton Leicestershire LE7 9JX

Tel: 0116 431 8284 **Mobile:** 0776 481 5991
Email: info@blinkoms.co.uk
Web: blinkoms.co.uk

VAT Registration Number: 988 7369 32

Infrastructure Security

The security procedures employed by Blink OMS are designed to ensure that no unauthorized access of user account details is possible. The threat landscape is an ever-changing environment, and we endeavour to keep our systems configured inline with industry best practice.

HTTPS

All Blink applications and other server to server communication are protected with SSL digital certificates issued by DigiCert Inc.

Zero Trust Policy

All infrastructure resources including databases, mail servers and internet servers are configured in line with our zero trust policies. By default, no permission is granted to any of our resources with configuration only being altered when agreement is reached that the change is necessary for appropriate Blink staff members to conduct their day-to-day operations to best support our customers.

Server Cybersecurity Solutions

Firewalls

All our servers are protected with industry leading firewalls which are configured in accordance with our Zero Trust Policy. No public access is available to any of our servers other than necessary ports and protocols to allow the delivery of HTML and SMTP services.

Anti-Virus

All or servers are protected with industry leading anti-virus software solutions which are updated automatically to ensure latest threats are detectable.

DDOS

How hosting partner provides a network level anti-DDOS attack solution to help protect all of our customers from DDOS attacks.

Database

The Blink databases do persist authentication information such as usernames and passwords. This sensitive information is always stored in an encrypted form to ensure that even with unauthorised access to the database a malicious actor could not gain access to the Blink application and assume the identity of another user.

General Data Protection Regulation (GDPR)

The Blink OMS application adheres to GDPR regulation. If not included with this document our GDPR statement is available upon request.

The Gables Church Lane
Hungarton Leicestershire LE7 9JX

Tel: 0116 431 8284 **Mobile:** 0776 481 5991
Email: info@blinkoms.co.uk
Web: blinkoms.co.uk

VAT Registration Number: 988 7369 32

Application Security

The security of user accounts within Blink is of utmost importance and every effort is made to ensure the integrity of the data contained within Blink is accurate and auditable.

User Impersonation

The Blink application does NOT support user impersonation. This means that it is not possible to login to the application and perform operations on behalf on another user even if that user's username and password are known.

Multi-Factor Authentication (MFA)

Each user account with Blink can be enabled to enforce MFA this process ensures that two authenticator methods are employed before access to Blink is granted. This configuration is performed by administrator level users within Blink and can be configured to use an Authenticator App or Mobile Phone SMS on a per user basis.

Blink OMS **strongly** recommends all users utilize MFA as part of their authentication process to prevent unauthorized system access by malicious actors.

Passwords

Users of Blink OMS are **strongly** encouraged to create strong passwords that exceed 12 characters in length especially when not enforcing MFA. Failure to create strong passwords can lead to unauthorized access by malicious actors.

The Blink application allows a logged in user to alter their own password. Once this password has been changed the only person who knows this password will be the user themselves. Once changed if the password is forgotten then the Forgot Password feature can be used from the login screen to provide access.

Planned Developments for Blink v4.55.0

As part of our on-going commitment to ensure that the Blink OMS application maintains data integrity for both the system owner and users whom access the application on their behalf, we have the following developments planned.

Auditing

A new feature being release as part of the Blink 4.55.0 release is the granular auditing of the examination and dispensing data elements within Blink. A comprehensive history of changes made to the examination and dispensing data will be recorded with an accompanying date and time stamp and who the logged in user was who made the change. This auditing data is not visible to any user with any level of authorization and can only be viewed if retrieved by the Blink development team at the request of an appropriate formal body e.g. PCSE or Police.

The Gables Church Lane
Hungarton Leicestershire LE7 9JX

Tel: 0116 431 8284 **Mobile:** 0776 481 5991
Email: info@blinkoms.co.uk
Web: blinkoms.co.uk

VAT Registration Number: 988 7369 32

User Change Notifications

A new feature being release as part of the Blink 4.55.0 release is the provision of a notification system that will send emails to any given user account that is altered. These emails will be sent each time a user account is changed regardless of the changers level of authorization and cannot be disabled via the configuration.