Flexxbotics Security

Flexxbotics

At Flexxbotics, we understand the importance of protecting our clients' information and data. That's why ensuring the security of our software is one of our main focuses. We incorporate security considerations throughout the design and development process and strictly adhere to policies and principles prioritizing the security of our software. This document outlines the general security policies and controls we have implemented to secure our clients' information.

OVERVIEW

All communication channels used by FlexxConnect are required to have a valid certificate, and we strictly enforce the use of SSL/TLS Protocol. All traffic routed via AWS uses TLS encryption 1.2 or higher and only HTTPS requests are allowed. Our token-based user authentication ensures that every request our software exchanges is authorized.

TLS Encryption

All traffic is encrypted with TLS (minimum version 1.2), and all requests are over HTTPS.

Security Provider

Our software leverages Auth0 for user authentication and permissions. Auth0 software is thoroughly vetted and is utilized by many companies, from small businesses to global enterprises. For their compliance certifications, please see https://auth0.com/security. Additional security measures, such as SSO, MFA or HIPPA, can also be configured based on our client's individual needs.

External and Internal Testing and Audits

We use an external service to conduct software penetration testing. Internal weekly reviews are performed to test the tools we utilize. If an issue is discovered, engineers immediately begin to resolve the issue.

Cloud Security

To safeguard your data, we rely on the robust security infrastructure of AWS. If any vulnerabilities are discovered, our Cloud platform automatically applies patches or updates, eliminating the need for manual updating and ensuring that our clients always have access to the most secure version of our software.

Employee Access

At Flexxbotics, we employ a strict zero-access model, where employees are only granted access to a resource when necessary. This also applies to our client's data: unauthorized employees can never access sensitive customer information. Only with direct customer approval can an authorized employee access any client data.

Data Durability

All hosted databases regularly have snapshots taken, so if a primary database ever fails, it can easily be restored.

Read our article on *Cybersecurity Best Practices for Connected Devices in Manufacturing*