SECURITY OVERVIEW - FULLPATH

Document overview:

This document outlines the information security processes and procedures at Fullpath.

Version: 202404.06

Yishai Goldstein, CTO, CISO

Table of Contents

Overview

This document outlines the information security policies, processes and procedures in place along with the security controls to ensure the safeguarding of data managed by Fullpath, and initiatives that measure compliance against delivery on those standards. The combination of these policies, standards and processes comprises the Information Security Program at Fullpath that is aimed at improving the security posture of the organization through early detection of security events, speedy resolution of incidents and non compliance, and continuous improvement of our security processes.

The purpose of information security at Fullpath is to:

1. Ensure the Confidentiality, Integrity, and Availability of data that Fullpath collects, receives, uses, and maintains.
2. Maintain compliance with contractual obligations
3. Maintain applicable data security regulations

General Information

Company Name

Fullpath Ltd.

Website

https://www.fullpath.com/

Products and Services

Fullpath provides a Customer Data and Experience Platform (CDXP). Fullpath's CDXP platform goes beyond a traditional CDP (Customer Data Platform) by using AI to analyze customer data and automate marketing campaigns. It personalizes the customer experience for car dealerships, helping them target potential buyers with relevant messaging and ultimately sell more cars..

Information Security Overview

The management of information security at Fullpath is outlined in the sections below.

ISO 27001 Certification

Fullpath has been fully certified since 2020 under the ISO:27001 standard and strictly abides by all information security requirements under the standard.

Data Types

Fullpath systems store and manage data gathered from a dealer's websites, DMS and CRM. All data, including any PII for customers is stored and maintained with consent from the dealers. Dealers have complete control over what data is shared with their vendors. If a dealer stops working with Fullpath, the dealer's data is removed from Fullpath's databases within 180 days. At any point whether a dealer is working with Fullpath or not, they may have their data removed from Fullpath's databases within 14 days, upon request.

Data Protection

Data privacy and security are of the utmost importance to Fullpath.

All data at rest in Fullpath systems is encrypted using a minimum of AES-128 encryption standard.

All data in transit uses secure protocols such as SFTP, FTPS, HTTPS, etc. protocols.

The information protection methodologies at Fullpath are implemented using guidance from the industry standard frameworks.

Access Control

Access to systems at Fullpath is controlled using centralized identity management (IDP and SSO) when possible. Access to all sensitive systems must be protected by MFA. In addition, we may also use Just in Time (JIT) access to systems. The principle of least privilege is employed for provisioning access to all systems.

By default, employees are not granted elevated accounts. Employees with a role that requires elevated privileges whenever practical, separate accounts will be provisioned and used only when such elevated privileges are needed.

All systems, whenever possible, require passphrases over simple passwords for employee end-users, privileged accounts, and service accounts have even more stringent requirements for passwords.

Access to systems must be audited at least annually.

Data Locations

Fullpath's servers and databases are located within the United States. The data is accessed by dealerships in the United States. Data requests from vendors outside the United States are fulfilled with consent from the dealers whose data is requested.

Service Hosting & Data Center

Fullpath infrastructure is hosted in AWS and GCP within the United States.

The AWS/GCP data centers are owned and operated by Amazon/Google and conform to industry standard security protocols for physical and environmental security.

Fullpath does not own and/or operate any physical data centers.

Corporate Office

The Fullpath facilities are not open to the general public and are access controlled for authorized employees and invited guests only. All access areas of Fullpath's HQ and development sites are covered with video surveillance.

Penetration Testing

Annual testing of publicly available products and services is performed by a third-party.

Vulnerability Management

Internal and external vulnerability scans of systems and services are performed at least monthly. The findings are analyzed and prioritized based on CVSS ratings and asset function. Remediation SLAs are established based on CVSS ratings – depending on rating, maximum remediation period is 30 calendar days.

Individuals with security responsibilities subscribe to alerts, notices, and feeds from key third parties to stay apprised of identified vulnerabilities and patch availability.

Social Engineering, Training, & Awareness

Social engineering campaigns are performed, and results are evaluated for individual and global training improvements. All employees undergo security training during on-boarding and well as at security awareness training at least annually. All employees must pass a security test at least annually. Developers must do additional security training at least annually. Additionally, notable landscape events are communicated to all employees.

Employee Workstations

All employees are provided with corporate owned laptops with centralized device management. All laptops have encrypted hard drives and user access control.

Remote Access

Fullpath employees my access systems using corporate devices only. Access is facilitated by SSO with 2-Factor Authentication.

Incident Response

The Fullpath Incident Response plan includes roles, responsibilities, communication, containment, eradication, and recovery considerations. Employee, IT, and Security Operations functions have a clear path for notification/escalation to the Incident Response Team.

Change Management

All significant change is managed by a fully documented process. The process includes documentation and communication requirements. All significant change requests are subject to a risk assessment and approval prior to implementation.

Third-Party Management

All third-party service providers/vendors are inventoried and classified. Full risk assessments are performed upon contract renewal or at least annually, for all critically classified third-parties.

End User

All Fullpath employees are required to abide by the following policies:

1. Employee Code of Conduct
2. Data Management Policy
3. BYOD Policy
4. Electronic Communications Policy
5. Remote Working Policy

Personnel

All US employees are required to comply with a criminal background screening prior to hiring. All employee access entitlements are least privilege and role based.

All employees are required to complete job and security training as part of initial onboarding.

Separated employees' access is revoked from all systems immediately.

Insurance

Fullpath carries a customary variety of insurance coverages.

Data & System Classification

A data classification program is in place at Fullpath where data is classified based on data type, subsequently systems are classified based on the highest data classification where data is transmitted, processed, or stored on the system. Control and handling requirements are based on the classification.

Endpoint Protection

Employee workstations/laptops are provisioned and managed utilizing centralized device management. They must be protected via MDR or next-gen antivirus.

All endpoints are must be managed, protected, and managed.

Software Development Life Cycle

Software development is conducted using an agile methodology. Testing - both manual and automated, peer review, and automated code analysis is used to ensure quality and avoid bug and security issues before deployment to production. Deployment to production is approved and audited through change management.

Identity Stores

Google Workspace is used as our main IdP, along with IaaC on AWS are implemented to enable access control, 2-Factor Authentication, and resilience

Network Security

All networks are architected with a principle of segmentation and strict access control. All firewalls have strict rule construction requirements including documentation and business justification.

Business Continuity

At least annually, a Business Impact Analysis is performed. Recovery Objectives are validated by Executive Management, and subsequently used to establish recovery priorities.

Backup

All systems and data are protected by a mixture of automated backup and snapshot processes that are aligned with established recovery point objectives.

Appendix

Abbreviations used in this document

PII	Personally Identifiable Information
SLA	Service Level Agreement
BYOD	Bring Your Own Device
CIP	Change Implementation Plan
SSO	Single Sign On
SFTP	Secure File Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
API	Application Programming Interface
UAC	User Access Control
JIT	Just In Time
DR	Disaster Recovery
BCP	Business Continuity Plan
DMS	Dealer Management System
CRM	Customer Relationship Management
MDM	Mobile Device Management
MDR	Managed Detection and Response
EDR	Endpoint Detection and Response
IdP / IDP	Identity Provider

Links

Fullpath Home Page: Digital Marketing & Customer Data for Auto Dealerships | Fullpath

on LinkedIn: Fullpath | LinkedIn