vaylens

Safety and security at vaylens

The constantly changing security requirements are implemented with great care during operation and further development at vaylens to guarantee our customers the best possible security when using our products.

vaylens GmbH

Ezzestraße 8
44379 Dortmund
Germany
help@emobility.software
vaylens.com

Management board: Jörg Lohr, Peter Hamela
Local court Dortmund: HRB 33903
VAT ID: DE352928826
Tax no: 314/5724/4552
HypoVereinsbank
IBAN: DE79 4402 0090 0023 1335 63
BIC: HYVEDEMM808

The security requirements for an IT platform are crucial to ensure protection against various threats and enable secure operation. Our cloud infrastructure is based on the latest security standards and includes the following essential security measures and requirements:

1. **Cloud Access Control**
    - **Authentication***: Our platform ensures that only authorized users have access by utilizing various authentication methods such as passwords, two-factor authentication (2FA), and biometric techniques.
    - **Authorization**: We use role-based access control (RBAC) to determine which resources and services an authenticated user can access.
    - **User Management**: User account management includes the creation, modification, and deletion of users as well as the management of their access rights.

2. **Data Integrity and Confidentiality**
    - **Encryption**: The data is encrypted both during transmission and at rest. We use TLSv1.2 or higher for transmission security.
    - **Data Integrity**: Mechanisms such as hash functions and digital signatures ensure the integrity of the data.
    - **Data Protection**: Measures to protect personal data are implemented in accordance with legal requirements such as GDPR.

3. **Network Security**
    - **Firewall**: Our infrastructure uses redundant firewall policies to control and secure incoming and outgoing data traffic.
    - **Intrusion Detection and Prevention Systems (IDS/IPS)**: Continuous monitoring and analysis of network traffic for suspicious activities and potential attacks.
    - **Virtual Private Network (VPN)**: External connections are secure and encrypted to ensure the safety of data transmission.
    - **Access Point Name (APN)**: Our specially configured APN infrastructure ensures that all mobile connections run over secure networks, providing additional protection.

4. **System and Application Security**
    - **Patch Management**: Regular updates of our software close known security gaps.
    - **Malware Protection**: Antivirus and anti-malware software are used to detect and remove malicious software.
    - **Security Policies**: We implement and enforce security policies and best practices for the development and operation of our software.
    - **Penetration Tests**: Regular penetration tests are conducted to identify and rectify vulnerabilities in our systems.

5. **Monitoring and Logging**
    - **Logging**: Security-relevant events and activities are recorded and analyzed.
    - **Monitoring**: Our platform undergoes continuous monitoring of interfaces to detect suspicious activities early.
    - **Incident Response**: Processes and tools for rapid response to security incidents are established.

6. **Security Awareness and Training**
    - **Training**: Regular training sessions raise employee awareness of security risks and practices.
    - **Awareness**: We promote a high level of security awareness within the organization to minimize human errors.

7. **Business Continuity and Disaster Recovery**
    - **Backups**: Regular backups of data and systems ensure recovery in the event of data loss or system disruption.
    - **Disaster Recovery****: Plans and procedures for the restoration of our systems and services after a severe incident are in place.
    - **Emergency Plans****: Our emergency plans are regularly tested to maintain business operations even during security incidents.

8. **Compliance and Auditing**
    - **Adherence to Standards**: We ensure compliance with relevant security standards and regulations and aim for corresponding security certifications.
    - **Audits**: Regular security audits continuously assess and improve our security measures.

9. **Physical Security in our Cloud**
    - **Access Control**: Our Cloud-Provider operates data centers globally, subject to strict access controls. Only authorized personnel have access to the data centers, and access is closely monitored and logged.
    - **Surveillance**: Our Cloud-Provider data centers are equipped with surveillance systems that operate around the clock to detect and prevent unauthorized access to the cloud infrastructure.
    - **Environmental Monitoring**: Our Cloud-Provider continuously monitors environmental factors such as temperature, humidity, and fire to protect the hardware within its cloud environment.

These comprehensive security measures ensure that our software platform remains robust, secure, and trustworthy.

* 2FA refers to our cloud infrastructure. This implementation is planned for the vaylens portal later.

** Plans and procedures are drawn up and integrated into the process landscape in a timely manner. Infrastructure requirements have already been implemented.