iGUIDE®

Made by PLANITAR INC.

Security information

A secure solution: Planitar's commitment to data protection

Transparency, Privacy and Security: Our Digital Trust focus

We prioritize the security and privacy of our customer's data. Our commitment to digital security and data privacy is evident across all our products and services. Our Digital trust strategy revolves around Information Security, Privacy and Transparency. We believe in transparency and strive to provide all the necessary information to establish a solid foundation before using Planitar's Platform, iGUIDE.

Planitar's information security program is developed to comply with industry-leading frameworks and standards such as International Standard Organization (ISO) 27001, the National Institute of Standard Technology (NIST) Cyber Security Framework (CSF) and incorporates control principles from Service Organization Control (SOC 2) Trust Services Principles and Criteria. Planitar's Information Security Manager oversees the overall security program and is supported by technical teams.

What is iGUIDE?

iGUIDE is our cloud-based software as a service (SaaS) product that simplifies the measurement and virtualization of properties and improves access to digitized property information.

Benefits include:

Comprehensive property documentation that can be experienced virtually 24/7/365 from anywhere in the world.

Time and cost savings by remotely accessing and exploring properties without the need for physical visits.

Enhanced collaboration and communication via sharing access to the digital property with anyone you choose, enabling efficient decision-making and streamlined workflows.

Planitar completed SOC 2 Type 1 examination

Annually, Planitar undergoes independent third-party audits against globally recognized standards like Service Organization Control (SOC 2) Trust Services Principles to guarantee our Client's data always remains protected. The examination yielded a 'no exceptions' result, the best possible result for a SOC 2 assessment.

Information uploaded to iGUIDE

The iGUIDE camera system (Planix) is used by an operator to capture the detailed property data (such as fisheye images and laser measurement data) required to make an iGUIDE.

An Operator moves the camera through a property to capture images and data from every room. Once done, the data is then exported from the camera system, before being uploaded to Planitar's cloud SaaS platform for processing.

Information security begins with the Planitar team

At Planitar, security is more than a set of rules and processes—it's part of our organizational culture. Our Engineering team has experience building secure SaaS applications that have scaled to millions of users.

Human Resources security

Planitar conducts background checks on all employees during the hiring process. Those handling restricted Customer data undergo reliability checks and must obtain Reliability Status clearance per the Government of Canada Standard Security Screening Process. Access to relevant systems or data is granted only after clearance.

We ensure that employees are aware of their obligations to protect company and Customer data. All employees sign a confidentiality and non-disclosure agreement (NDA) as part of their employment contract. Employees also receive and accept company policies, which stipulate their responsibilities around the acceptable use of IT assets, as well as information security and confidentiality.

Security and privacy training

Every Planitar employee receives security and privacy awareness training, both as part of their onboarding and as a refresher on an ongoing basis at least annually. Security and privacy awareness training covers topics, such as:

- General information security overview
- Phishing awareness and prevention
- Security incident management
- Confidentiality requirements
- Data privacy

Information security policy and procedures

Planitar's management has adopted the implementation of internal policies and procedures to ensure that security best practices are followed and to facilitate continuous improvement while providing overall program governance.

The Information Security Policy (ISP) summarizes the top-level controls that are to be followed to protect Planitar's digital assets. This policy is communicated to all employees, who are required to attest to understanding and adhere to its requirements.

Infrastructure Security

Planitar's cloud infrastructure is hosted and managed on Amazon Web Services (AWS) across multiple availability zones located in Canada and the United States of America to support fault tolerance, high availability and disaster recovery.

Platform Architecture

We've built Planitar's cloud to support both multi-tenant and single-tenant architectures, applying common and consistent management processes and controls to all customers. Customer data is separated through strict coding standards, code reviews and database design.

Encryption

We protect your data both in transit and at rest. Customer data is transferred to Planitar over a Transport Layer Security (TLS 1.2) connection and data stored at-rest is encrypted with Advanced Encryption Standard (AES 256).

High availability

Planitar designed its infrastructure to provide high availability, and all critical infrastructure components are redundant across multiple AWS availability zones. We have deployed Web servers and databases in multiple availability zones, each consisting of one or more discrete data centers, with fully redundant power, networking and connectivity housed in separate secured facilities.

Access management

Senior Engineering team members oversee access rights in the production environment. Access privileges are restricted to authorized individuals, and all requests are documented and approved through a change management log. Regular manual access reviews are conducted as an additional safeguard, ensuring that administrative access to production systems aligns with approved roles and responsibilities.

Security monitoring

We have implemented comprehensive logging using AWS CloudWatch to monitor and analyze in-scope systems for threat vectors and potential security breaches. Our technical teams are promptly alerted of threat vectors and potential security breaches through our monitoring and alerting platforms. We also utilize an endpoint detection and threat response system to monitor on-premise IT infrastructure accessing restricted Customer data.

Our dedicated managed security operations center (SOC) provides 24x7 monitoring and remediation for identified intrusions on Planitar's on-premise IT infrastructure.

Software development lifecycle

Developers in the engineering team perform source code peer reviews encompassing, functional and performance testing of all major application changes before implementing them into the production environment. Development and testing activities are performed in separate environments that are logically separate from production to ensure that changes made within the test environment do not impact the production environment.

Network segregation

Network segregation via a virtual private network (VPC) is enforced by AWS to ensure each customer utilizing its IaaS service is isolated at a network level. Additionally within Planitar's VPC, network segmentation has been configured via security groups and access control lists to keep internal portions of our cloud networks segregated from the public or nonessential internal access.

Data retention

Upon written request or confirmed digital request, Planitar will delete all Customer data from the production environment within 30 business days or automatically after service termination, unless otherwise instructed or contractual obligated not to. System-wide encrypted backups are maintained for a revolving period to meet our obligations under respective Data privacy regulations (PIPEDA, GDPR) and Customer service agreements.

Business Continuity and Disaster Recovery (BCDR)

Planitar has implemented a BCDR plan to ensure that we meet business and availability requirements. Our cloud platform has been designed to maintain contractually mandated recovery objectives and tests are regularly conducted (annually in line with best practices) by the Engineering team to ensure compliance with agreed recovery commitments.

Physical security

Access to our office in Ontario, Canada is controlled by a tiered proximity access fob system. Depending on the team member's internal clearance level, entry to specific rooms where sensitive information is accessed and/or processes within the facility are disabled. Only authorized team members with appropriate clearance levels are enabled to enter secure operational zones.

A physical deterrent control, alarm systems and closed-circuit television (CCTV) surveillance cameras are strategically installed on the premises.

Physical access to our cloud platform managed by AWS is also controlled through key card proximity systems. Access requires two-factor authentication with a biometric system and key card.

Digital trust is a shared responsibility

To support our transparency goals, Planitar has identified key responsibilities of external sub-service organizations and Customer entities that are mandatory in guaranteeing the success of our Digital Trust strategy.

Sub-service organizations

Planitar utilizes AWS Infrastructure-as-a-Service (IaaS) platform to provide computing (virtual hosts), networking and storage. Maintaining the operational security of this facility is solely the responsibility of AWS. This facility hosts Planitar's multi-tenant and dedicated SaaS platform that hosts APIs, support and administrative web applications. AWS does not have logical access to Planitar's data.

Physical security and environmental controls within the US and CA availability zone where Planitar hosts its cloud platform, are managed completely by AWS, summarized as follows:

Fire detection and suppression systems: Fire detection and suppression systems, including pre-action dry pipe, hand-held fire extinguishers, smoke detectors, and fire alarms. The fire detection and suppression systems are tested on an annual basis.

Backup power: This included uninterruptible power supply (UPS) units and redundant generators, power distribution units (PDU) and electrical panels. UPS units are located in dedicated areas. The primary UPS is tested periodically under load conditions and performance results are monitored. Data facilities are equipped with generators that automatically supply power to the facility in the event of outside power failure.

Heating and cooling: HVAC mechanisms, such as computer room air conditioning (CRAC) units, computer room air handlers (CRAH), chillers, and temperature and humidity monitoring and control. HVAC equipment, depending on the type, is maintained at a quarterly frequency.

Firewalls: Network devices, including firewalls and other boundary devices are in place to control communications at the external boundary of the network. This includes devices solely managed by AWS to control all network traffic to the cloud IaaS platform. Additionally, network access control mechanisms are managed by Planitar to specifically monitor and control network traffic sent to Planitar's VPC.

Our primary hosting provider, AWS, complies with various international security and privacy standards, including; ISO/IEC 27001:2013, SOC 1, SOC 2, SOC 3 and GDPR. Find out more about security, privacy and compliance at AWS here.

Customer entities

We prioritize the trust our customers have in our products and services. Our Digital Trust programs are regularly assessed and strengthened to align with industry best practices. It is crucial to emphasize the shared responsibility between Planitar and our customers in operating our platform securely. While we are responsible for platform security, customers also play a role in ensuring security while utilizing our platform, as outlined:

Access management: Customer entities are responsible for ensuring that access to Planitar's platform is restricted to only authorized personnel. Each person should be given a unique set of access credentials (username and password) and sharing of credentials with colleagues should be prohibited. Additionally, each authorized personnel should be given the level of privileges that is commensurate with their business function following the principles of least privilege access.

Sensitive data: To leverage the services offered by Planitar, personnel in Customer entities are not required to share or upload any information outside iGUIDE generated data (camera fisheye images, laser measurement or property meta-data). To avoid the export of personally identifiable or sensitive information, rooms should be sanitized prior to scanning with the iGUIDE camera system, or alternatively, image files should be sanitized by the Customer entity prior to uploading to Planitar's cloud platform.

Safeguarding iGUIDE exports: Once Customer entities have completed scans using the iGUIDE camera system, safeguarding iGUIDE-generated data (camera fisheye images, laser measurements or property meta-data) stored on physical media throughout its life cycle is the responsibility of the Customer entities. Where it is stored, how long it is kept and when it is disposed of are all decisions that are at the discretion of the Customer entities.

Trust Planitar: Your secure and reliable digital partner

Planitar prioritizes the security and privacy of our customer's data. Our information security programs align with leading frameworks such as ISO 27001, NIST CSF, and SOC 2. With transparency as our foundation, you can trust Planitar for secure and reliable solutions in the digital landscape.

To further discuss our Digital Trust program, please contact us at:

1 844 568 1723
sales@planitar.com

About us

Founded in 2013, in Kitchener, Ontario, Canada, Planitar Inc. is the maker of iGUIDE, a proprietary camera and software platform for capturing and delivering immersive 3D virtual walkthroughs and extensive property data.

Why iGUIDE

iGUIDE is the most efficient system to map interior spaces and features accurate floor plans, measurements and reliable property square footage. By integrating floor plans and visual data, iGUIDE provides an intuitive and practical way to digitally navigate and explore built environments.

Contact us

sales@planitar.com
1 844 568 1723
goiguide.com

560 Parkside Drive,
Unit 401, Waterloo, ON,
Canada N2L 5Z4

iGUIDE®