Imagineer Technology Group, LLC
Security Policy

Effective: May 1, 2018

We understand how important the security, privacy and confidentiality of your data is to you and your teams and work to the best of our abilities to ensure your expectations are met. Please make a point to review the information below regarding our current policies and practices, along with our Privacy Policy, Data Processing Addendum, Acceptable Use Policy, and the terms and conditions associated with our service Agreements. This is a living document and we will update it as our service evolves and industry practices change. Below are some details on our security practices.

Security
As a company, we use Imagineer services (Clienteer, Synap, WebVision) for managing all of our customer communications. Ensuring that all of Imagineer services (Clienteer, Synap, WebVision, Fundinsight) remains secure is vital to protecting our own data. The security of your information is required for our success as a business.

Information security policies of the Imagineer are reviewed at least annually and refined as necessary to keep current with modern threats and in line with updates to broadly accepted international standards.

Imagineer follows a mandated set of employment verification requirements for all new hires, including supplemental employees. These standards also apply to wholly owned subsidiaries and joint ventures. The requirements, which may be subject to change, include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks if the candidate previously worked for a government entity. Each Imagineer employee is responsible for implementing the above requirements in its hiring process as applicable and permissible under local law.

Imagineer employees are required to complete security and privacy education annually and certify each year that they will comply with Imagineer ethical business conduct, confidentiality, and security requirements, as set out in Imagineer Acceptable Use Policy.

Security incidents are handled in accordance with Imagineer incident management and response policies, taking into account data breach notification requirements under applicable law.

The core functions of Imagineer cyber security incident management practice are conducted by Imagineer Compliance Group (ICG). ICG is managed by Imagineer Chief Information Security Office and is staffed with incident managers and outsourced forensic analysts. National Institute of Standards and Technology, United States Department of Commerce (NIST) and ISO guidelines for computer security incident handling have informed the development and remain the foundation of Imagineer incident management processes.

The ICG coordinates with other functions within Imagineer to investigate suspected incidents, and if warranted, define and execute the appropriate response plan. Upon determining that a security incident, including a data breach, has occurred that affects Company, Imagineer Contracting Party will notify Company within 72 hours of being aware of the breach. For high-risk events, Imagineer will notify customers without undue delay (Article 31). The notification given will provide at least:

- Nature of the breach
- The name and contact details of the incident response manager assigned to the incident
- If known, the likely consequences of the breach

- The current measures taken or proposed to be taken to address the breach and mitigate its adverse effects.

Encryption
To be considered approved for use by Imagineer, algorithms, implementations (e.g., software modules or libraries), software or other cryptographic components must appear on the Approved Cryptosystem List, available from the security team (ICG – Information Compliance Group). Modules that are certified to comply with Federal Information Processing Standard (FIPS) 140 (at level 2 for software modules or level 3 for hardware modules) are considered preapproved for use provided that cryptographic algorithms and parameters approved by the US National Institute of Standards and Technology (NIST) are employed and the modules are configured in NIST mode.

Approved ciphers include AES 256, SHA-256 and RSA employing keys of at least 2048 bits or greater. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric cryptosystem keys must be of sufficient length to yield equivalent strength. These key-length requirements will be reviewed annually.

Additionally, data is encrypted at rest in Imagineer's data stores for Clienteer, Fundinsight, and Synap.

We use a third-party, industry-accepted Payment Provider to securely process credit card transactions and store payment credentials.

We monitor the security community's output closely and work promptly to upgrade the service to respond to new vulnerabilities as they are discovered.

Secure Physical Location, Entry Control
Imagineer maintains physical security standards designed to restrict unauthorized physical access to offices. Imagineer uses AWS, Azure and Cyxtera and their data centers are limited controlled access, and monitored by surveillance cameras. Access is allowed only by authorized personnel.

https://aws.amazon.com/compliance/iso-27001-faqs/ and
https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf,
https://servicetrust.microsoft.com/ViewPage/HomePage,
https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide

Delivery areas and loading docks where unauthorized persons may enter the premises are strictly controlled. Deliveries are scheduled in advance and require approval by authorized personnel. Personnel who are not part of the operations, facilities, or security staff are registered upon entering the premises and are escorted by authorized personnel while on the premises.

Activity Logging, Input Control
Imagineer policy requires administrative access and activity in the computing environments to be logged and monitored, and the logs to be archived and retained in compliance with Imagineer records management plan. Changes made to production are recorded and managed in compliance with Imagineer change management policy.

Upon termination of employment, employees are removed from the access list and required to surrender their access badges. Use of access fobs is logged.

Service Integrity & Availability Controls
We understand that you rely on our products to work. We're committed to making them highly-available, ultra-reliable services that you can always count on. We build systems that tolerate the failure of individual computers or whole datacenters, keep many copies of your data online for redundancy,

practice disaster-recovery measures often, and always have staff on-call to quickly resolve unexpected incidents.

Imagineer undergoes penetration testing and vulnerability scanning from time to time in accordance with its best practices. Penetration testing and vulnerability scanning, is also performed by Imagineer and authorized independent third parties from time to time. Modifications to operating system resources and application software are governed by Imagineer change management policies.

Imagineer maintains working network firewalls to protect data accessible via the internet and will keep all Customer Data protected by the firewall at all times. Changes to network devices and firewall rules are also governed by the change management policies and are separately assessed for security risk prior to implementation.

Imagineer data center services within AWS, Azure and Cyxtera support a variety of information delivery protocols for transmission of data over public networks, such as HTTPS, SSH, and SSL. Imagineer systematically monitors production data center resources 24x7. Internal and external vulnerability scanning is regularly conducted by authorized administrators to help detect and resolve potential exposures.

Imagineer has business continuity and disaster recovery plans, which are developed, maintained, verified, and tested. Security configuration and patch management activities are performed and reviewed regularly. Imagineer infrastructure is subject to emergency planning concepts, such as disaster recovery and multiple AWS or Azure servers and a secondary data center to Cyxtera, as the case may be, available in regions throughout the country. Business continuity plans for Imagineer infrastructure are documented and regularly revalidated.

Imagineer maintains best of breed anti-virus software and scanning technologies, and regularly updated signature files, to ensure that all operating systems, software and other systems hosting, storing, processing, or that have access to data and are known to be susceptible or vulnerable to being infected by or further propagating viruses, spyware and malicious code, are and remain free from such viruses, spyware and malicious code. Imagineer will mitigate threats from all viruses, spyware, and other malicious code that are or should reasonably have been detected.

Confidentiality

We regard the information you share within your Imagineer team as private and confidential to your team. We place strict controls over our employees' access to internal data and are committed to ensuring that your data is never seen by anyone who should not see it.

While the operation of the Imagineer services would not be possible unless there were some technical employees with sufficient system permissions to enable them to access and control software that stores and indexes the content you add to your instances of the Imagineer services, this team is kept purposefully small and are prohibited from using these permissions to view customer data unless it is necessary to do so.

All of our employees and contractors are bound to our policies regarding customer data and we treat these issues as matters of the highest importance within our company. If, in order to diagnose a problem you are having with the service, we would need to do something that would expose your personal communications to one of our employees in a readable form, we will ask for your consent prior to taking action.

There are limited circumstances when we ever share customer content without first obtaining permission. These are clearly outlined in our Privacy Policy.

Privacy
A fundamental privacy principle we abide by is that by default, anything you post to Imagineer is private to your team. That is, viewing the messages and files shared within a specific team requires authentication as a member of that team. Imagineer has a comprehensive Privacy Policy that lays out our approach to privacy. Please read it.

If you are using any of Imagineer's services in a workplace or on a device or account issued to you by your employer or another organization, they will almost certainly have their own policies in place regarding storage, access, modification, deletion and retention of communications and content. Please check with your employer or team administrator about what policies they have in place regarding your communications and related content.

Compliance
Imagineer information security standards and management practices are aligned to the ISO/IEC 27001 standard for information security management. Assessments and audits are conducted regularly by Imagineer to track compliance with its information security standards. Additionally, independent third-party industry standard audits are performed annually on all Imagineer production systems maintained in AWS, Azure and Cyxtera data centers.

Experienced Team
Even before Imagineer, our team has been putting services on the internet for a long time. We're not perfect but we're pretty good at it. Our product engineering and technical operations team members are experienced and keep their skills up to date as industry best practices evolve. We've coded, tested and administered services running on thousands of physical servers in data centers around the world and we bring the collective wisdom that comes with many decades of secure practice to the operation of Imagineer's services.

We know how important these issues are to you and can honestly tell you they are equally important to us. The security, privacy and confidentiality of your information are core to our success as a business. Rest assured that we will continue to be proactive and diligent in ensuring its safety.
If you have additional questions regarding data privacy, security or confidentiality, we'd be happy to discuss them with you. Email us at privacy@itgny.com and we will respond as quickly as we can.
If you believe you have found a security vulnerability on any of Imagineer's services, we encourage you to let us know right away. We will investigate all legitimate reports and do our best to fix any problems quickly.