Security Practices at Stratasys/ GrabCAD

July, 2021

Contents

Security Introduction 3

People Security Practices 4

- Human Resources Security 4
- Physical Security 4
- Authentication 4

Process and Technology Security Practices 5

- Secure software development policies and infrastructure 5
- System change control procedures 5
- Technical review of applications 5
- Secure system engineering principles 5
- Secure development environment 5
- Outsourced development 6
- System security testing 6
- System acceptance testing 6
- Business Continuity/Disaster Recovery (BCDR) 6

Built on Secure Technology 7

- GrabCAD Print 7
- GrabCAD Shop 7
- Compliance 7

Data Security Practices 8

- Ensuring Proper Data Protection Controls 8
- Data Collection 8
- GrabCAD Print 9
- GrabCAD Shop 9
- Data Segregation 9

GrabCAD Print Summary of GrabCAD Print application and printer data collection 10

GrabCAD Shop Summary of GrabCAD Shop application and printer data collection 11

Commonly Asked Security Questions (FAQ) 12

Disclaimers, Advisories And Resources 15

Security Introduction

Cybersecurity is increasingly critical to every organization, especially for those with manufacturing operations and smart, connected equipment such as 3D printers and other IoT devices. Much attention has been given to IP theft, ransomware and malware, threats that are costing organizations billions of dollars annually. But these aren't the only concerns.

According to the authoritative 2020 Verizon Data Breach Incident Report more than a quarter (27%) of breaches at manufacturing organizations (NAICS 31–33), involved industrial espionage efforts. Organizations outside of the financial sector sometimes feel they won't be targets for cyberattacks but they are and the stakes are high. That's why the Stratasys software team has always prioritized good security practices.

> The subject of this paper is the GrabCAD 3D Print Platform (GrabCAD), which is developed by the Software Business Unit (SWBU) within Stratasys. GrabCAD provides application software and services to Stratasys customers who:
>
> 1. Program parts for 3D printing from digital CAD files.
> 2. Manage shared office, model shop and manufacturing environments.
> 3. Collect operational data on printer usage, and integrate it with other enterprise software applications, to share information with other users.

The GrabCAD Platform is made up of several products including GrabCAD Print, GrabCAD Shop, GrabCAD Software Development Kit (SDK), and GrabCAD Community and will be further expanded in the future. The focus of this document is to communicate the security practices that Stratasys has implemented and follows.

Stratasys utilizes a three layered approach to developing secure software for our products and managing good security practices: People, Process and Data Security to ensure development of secure software and practice of good internal controls.

People security involves making sure that everyone at the company, including those that develop software solutions, is aligned with security goals and prepared with the correct knowledge and skills to maintain and develop secure products.

Process security is the way Stratasys does business, the way it creates and delivers its products and services to support and reinforce security.

Data security ensures that any personal, usage or hardware data collected from our customer's use of Stratasys software is securely transferred and stored, in a strictly access controlled environment.

People Security Practices

Human Resources Security

Mandatory security training, phishing and other cybersecurity courses need to be completed on a regular cadence (once a year) by all employees. Employees have access to these IT related courses in the Stratasys Academy. Additionally, Stratasys is registered for ITAR and has established compliance and controls for employees.

All new employees and contractors who work on software are onboarded and trained on our Standard Operating Procedures (SOP), GrabCAD technology and security measures. They are assigned a mentor and a project team to support and guide them in their work and to stay apprised of security best practices. At the time of onboarding, new employee access to software tools, source code and related systems is also controlled and granted by internal admins.

Similarly, when individuals' employment with Stratasys is terminated, a series of rigorous steps ensure that access is revoked promptly, physical or intellectual property is accounted for (devices are wiped and returned), and access to facilities (key card access) is concluded.

Physical Security

Video monitoring is present for all ingress and egress points. Visitors from customer organizations, vendors or other third parties are always escorted and their presence is recorded and logged.To ensure that customer-specific proprietary information is not circulated freely, only designated and authorized employees can access specific physical and logical areas within Stratasys.

Authentication

Stratasys follows NIST SP 800-63 Digital Identity Guidelines for employees (developers and other staff). As a result, employees are required to have strong passwords and multifactor authentication (MFA) before they can access software tools for development and delivery. In addition, passwords are regularly monitored against compromised passwords on the dark web. Stratasys encourages users to implement similar controls with their GrabCAD user accounts.

All these steps combine to ensure that Stratasys employees are working to support high-levels of security required at all times.

Process and Technology Security Practices

Secure software development policies and infrastructure

Processes ensure efficient developer workflows and adherence to proper and secure development practices. Ongoing practices and processes to further support security measures include:

- An annual and quarterly planning process that identifies high-level themes and initiatives and captures work that teams will focus on.
- Use of Agile development to plan sprints in Epic and Story format. Stories are specified with security requirements built in.
- Use of secure tools to manage processes and code base including Jira® for backlog management and Github for code management.
- Code reviews by peers to ensure good code quality and security practices.
- Use of modern, secure technologies, including programming languages, third-party services like AWS, and third-party components (eg, identity management).
- Disaster recovery procedures.

System change control procedures

Prior to its start, every project has a specification that must be adhered to. Security is an important aspect of the start of new feature development or any other project. Development groups operate as scrum teams with a scrum master. Every issue either internal or from customers is logged as a ticket in Jira®, prior to being worked on to ensure traceability. Ticket implementation is reviewed by one or more peers and a QA process verifies correctness and the presence of appropriate tests before it is marked as complete.

Technical review of applications

The updated software goes through automated software checks for early detection of errors. Market documents and functional specifications are handled and tracked with Jira® Software Themes, Initiatives, and Epics to respond to change, report progress, and conform to plan.

Secure system engineering principles

Stratasys maintains Standard Operating Procedures (SOP) document that defines the entire development process which is followed by each developer. SOP is part of every new employees' onboarding process.

Secure development environment

To further ensure that software development practices facilitate security, GrabCAD subscribes to GitHub.

- Source code is maintained in GitHub repositories.
- Access to GitHub is authorized as part of the onboarding process.
- Access to source code in GitHub is by named user only.
- Each change to source repositories in GitHub can be traced to a user and a specific date and time when it was made as an audit trail.
- Source code changes can be reverted, if necessary.
- As part of the development process, developers are expected to write unit tests and update smoke tests (a.k.a. build verification tests), as necessary.
- Any source code change is controlled through a change control process.

Process and Technology Security Practices

- Change control processes require rigorous automated and manual testing before a developer's source change branch can be merged to master.

Security vulnerabilities in open source packages and other relevant vulnerabilities are addressed in the next software release, or sooner, if the issue is deemed critical. Updated software is also exposed to static application security testing (SAST) tools to find any potential security vulnerabilities.

Outsourced development

As mentioned before, any developer including outsourced developers / contractors are trained to follow our SOP, and security measures. They work in a team structure, and follow sprint planning, code reviews, testing prior to release, along with the internal teams.

System security testing

Cloud products undergo a further set of analysis. This includes annual penetration testing, which is a simulated cyber-attack by a renowned external agency to check for exploitable vulnerabilities. Additionally, Stratasys subscribes to the Hackerone bounty program, which engages a community of external, ethical hackers to further ensure the product is secure.

Finally, the cloud software also undergoes runtime analysis for security checks using dynamic application security testing (DAST), which simulates external attacks while the application is running.

System acceptance testing

System acceptance is performed by a dedicated QA team to ensure stability and quality of the application prior to its release.

Business Continuity/Disaster Recovery (BCDR)

Stratasys has a business continuity plan for situations where personnel cannot access company facilities in person. This plan has proved its value during the COVID-19 pandemic as Stratasys employees worked remotely during the pandemic, with zero downtime in GrabCAD systems.

Built on Secure Technology

In addition to managing security practices via People and Processes, security practices are also addressed with underlying technology choices. The GrabCAD Platform (and related products) is a SaaS developed, deployed and delivered via Amazon Web Services (AWS).

Using AWS allows Stratasys to scale software development and deployment throughout the GrabCAD Platform. Access controls and continuous monitoring capabilities enable good health and minimal downtime of all products. AWS's container based systems guarantee maximum software performance, data-retrieval speeds and user experience.

Finally, AWS automatic task management and virtual machines allow Stratasys to consistently run tests on production code and environments to protect against regressions, enabling the software team to deploy new features and software updates efficiently.

Stratasys consistently manages physical security, logins and password management, account management, and access control across the GrabCAD 3D Print platform. However, certain products in the platform are deployed differently based on the relevant 3D printing workflows. For example:

GrabCAD Print

GrabCAD Print is the print preparation desktop application that is used to send CAD files over a LAN to the printers (if needed, over the cloud to Printers outside the network). With the LAN connection to the printers, it is also used to monitor the printer statuses, queues and schedules.

Finally, it can also be taken completely offline to block any communication outside a customer's network firewall if needed or preferred (one of the many instances where different security options can match different needs).

GrabCAD Shop

GrabCAD Shop is a web based work order management application designed to support 3D printing / model shop collaboration between colleagues, no matter where they are. Users upload CAD files and relevant data to their virtual model shop, to be fabricated by shop operators and administrators, based on the technologies and inventory available in that company's model shop.

To improve 3D printing workflows, and to reduce latency to a minimum, all GrabCAD Shop data is stored securely on the AWS cloud.

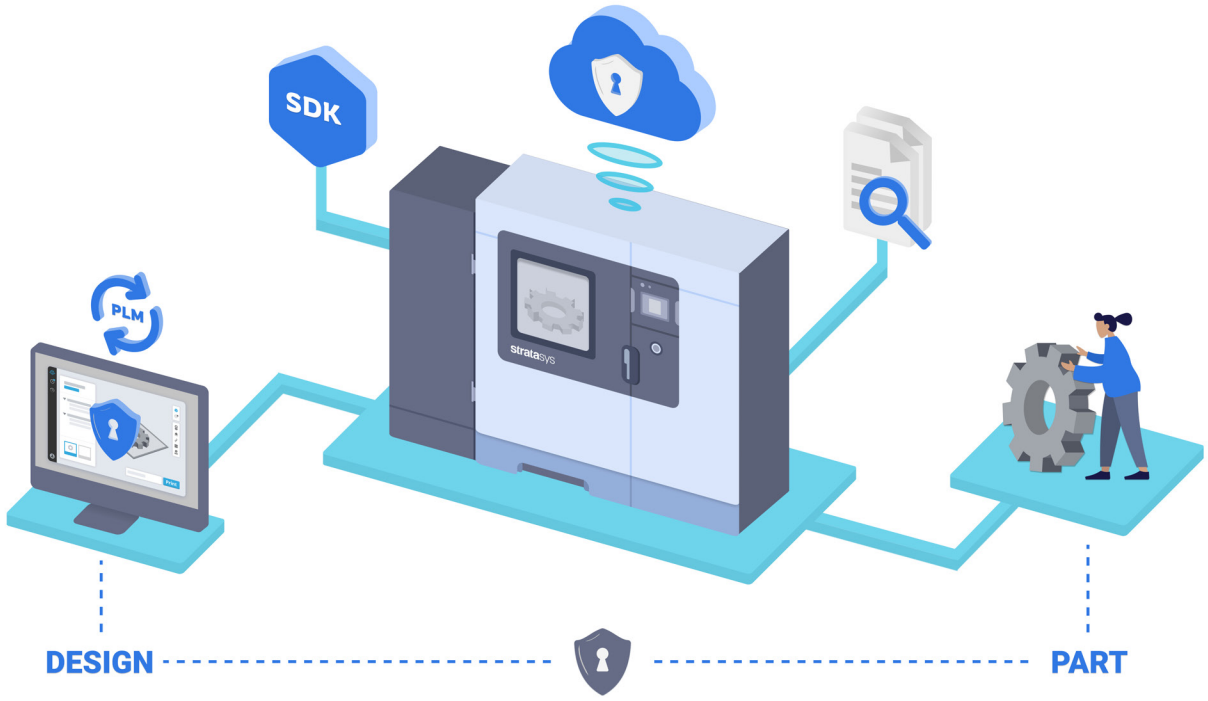
Compliance

By relying on AWS, Stratasys leverages the various security standards and compliance certifications that AWS supports, more than any other comparable platform. This includes FedRAMP, GDPR, FIPS 140-2, and NIST 800-171.

Compliance with California Consumer Privacy Act (CCPA) and Family Educational Rights and Privacy Act (FERPA) is generally the responsibility of each individual user organization, though, where possible, Stratasys aligns its practices with these measures.

Stratasys also conforms to the requirements of the EU General Data Protection Regulation 2016/679 (GDPR).

Data Security Practices



Ensuring Proper Data Protection Controls

The third and final layer of Stratasys' security program is focused on Data Security Practices.

GrabCAD cloud applications are front ended by a web application firewall (WAF), an important type of application firewall that filters, monitors and even blocks HTTP traffic with a web service. WAF can prevent attacks from exploiting known vulnerabilities, such as SQL injection, file inclusion, improper system configuration or even cross-site scripting (XSS).

In this way, WAF can help stop or curtail distributed denial-of-service (DDoS) attacks and other threats identified by OWASP (the Open Web Application Security Project). That's the proactive, day-to-day activity that helps keep GrabCAD users safe. But Stratasys also undertakes periodic longer-term activities, including a Disaster Recovery plan relevant for supporting GrabCAD products. These plans are practiced once a year.

Amazon Web Services (AWS) data is stored redundantly across multiple devices in distributed and environmentally controlled facilities. AWS infrastructure and controls are subject to annual SAS-70 Type II audits and AWS information security. AWS management processes and controls have achieved ISO 27001 certification. Encryption is utilized while data is in transit between the user's company network and AWS server. Data at rest is also encrypted.

Data Collection

When Stratasys customers sign up for a GrabCAD account, they are asked for first and last name, location-country and state/region, telephone number, verified email address, and role in their company (e.g. engineer, designer, operator, student).This personally identifiable information (PII) is used for communication and support.

Data Security Practices

GrabCAD Print

GrabCAD Print collects application and hardware usage information associated with a user's email. The data collected is used to provide support services and for enabling web based printer / material usage, reporting, printer history, and remote and mobile monitoring functionality.

Application usage data collected include when the customer opened the program last, when the customer printed last, how many total trays a customer has printed, what materials a customer has printed jobs with, print start times, print stop times, total printing time, and errors encountered, and event counts of certain features used in GrabCAD Print to aid feature development.

Additionally, hardware usage data also includes printer statuses, history, owner, materials information to enable the aforementioned web monitoring and reporting functionality.

Users can anonymize or disable this data collection and functionality in GrabCAD Print under "File>Preferences> Privacy". Regardless of these preferences, no CAD or proprietary design metadata is ever collected.

GrabCAD Print can also operate in offline mode where it will not communicate any of the previously mentioned data. This mode is currently used by ITAR-compliant customers. They trust that their interaction with the software is safe and that their files and proprietary data will stay in their network.

GrabCAD Shop

GrabCAD Shop allows users to upload their CAD files through a secure portal for 3D printing. It collects and securely stores the data uploaded by customers on AWS, to allow operators and other users to collaborate and access their own Shop's data from anywhere.

Data uploaded by one customer is logically separated from others', so customers can access only their own proprietary data at any time.

Data Segregation

As mentioned above, like many other organizations that work with multiple entities, customer data is logically separated from that of other customers within the GrabCAD shared infrastructure, so there is no mixing of data. This multi-tenant architecture ensures both higher availability and resilience while also providing assurance of data security for each individual organization.

GrabCAD Print

Summary of GrabCAD Print application and printer data collection.

Product	Privacy Settings	Personal Data collected at signup or on GrabCAD.com	User Submitted Data	Application Usage Data	Printer Usage data
GrabCAD Print	Online personal data enabled (allows GrabCAD to identify users)	Name Email Company Details Sign up and login required to use Print	No CAD files are uploaded to GrabCAD servers. Tray images may be uploaded for a limited time for collaboration	When user logs in User actions in GrabCAD Print	Printer serial numbers identifiable Job related metadata (job name, owner name, print time, duration, estimations, material information, tip information, printer temperature and other related printer health data)
	Online-Anonymous-Data Only	Email Company Details Sign up and login required to use Print	No CAD files are uploaded to GrabCAD servers. Tray images may be uploaded and stored for 30 days to allow collaboration	Anonymized login event Anonymized user actions	Printer types identifiable No printer serial numbers Job related metadata (job name, owner name, print time, duration, estimations, material information, tip information, printer temperature and other related printer health data) Does not include part names and job owner
	Offline - No Data Collected	Sign up and login required for initial download updates only. Not required during use in offline mode.	None	None	None

GrabCAD Shop

Summary of GrabCAD Shop application and printer data collection.

Product	Privacy Settings	Personal Data collected at signup or on GrabCAD.com	User Submitted Data	Application Usage Data	Printer Usage data
GrabCAD Shop	Not Applicable	Name	Upload files	When user logs in	None
		Email	Comments	User actions in GrabCAD Print	
		Company Details	Shop metadata		
		Sign up login and license required to use Shop	Thumbnails	Machine types added by the administrator	
				Materials used	
				Users invited	

Commonly Asked Security Questions (FAQ)

Authentication	**Q:** What password controls are enforced for employees / developers of the software?	**A:** Strong passwords (NIST SP 800-63 Digital Identity Guidelines) and MFA is required for all developers.
Information Security Program	**Q:** What roles and responsibilities are assigned to manage the security program?	**A:** Stratasys has a CIO who oversees the corporate and information security functions. Within the Stratasys Software Business Unit (SWBU), there is a designated Security Officer.
	Q: Is an Information Security Policy maintained with related standards, guidelines, and procedures for all employees and external parties? (e.g., contractors, affiliates, suppliers, partners)	**A:** Yes. SWBU maintains a Standard Operating Procedures (SOP) document for procedure and guidelines for all employees and external parties.
Access Management	**Q:** Are procedures for user account provisioning / deprovisioning, management, and data access control established and maintained?	**A:** Yes. SWBU maintains a SOP document that covers these topics. Data and account access is granted on a “need to know” basis, and requires approvals and business reasons prior to authorization. Data access is also MFA enabled. Separation/termination processes are handled and governed by Stratasys HR policies.
Systems & Security Hardening	**Q:** Are all versions of operating systems and application software current, with security patches, anti-virus software regularly installed? Is an anti-phishing / spam protection and reporting process established?	**A:** Yes. SWBU subscribes to regular OS and security upgrades and has enabled Virus/ malware scan to run in background on our systems to keep associated signature files upto date. Yes. The Stratasys MIS department has anti-phishing / spam protection and mandatory training courses for all employees.

Commonly Asked Security Questions (FAQ)

Information Protection Security	**Q:** Is data from the software encrypted in transfer and rest? How are employees trained to protect customer sensitive data?	**A:** Yes, Data from the GrabCAD Software is always encrypted in transit and at rest in AWS (using the latest TLS encryption methods). All Stratasys employees have to complete mandatory annual security training which covers best data management practices (Eg: Discouraging / Prohibiting the use of removal media from any data storage)
Physical Security	**Q:** What physical access controls are established in Stratasys offices?	**A:** Offices are physically secured for access. Offices maintain video monitoring at ingress/ egress points and enforce badge access. All visitors are logged and escorted while in the office.
Business Continuity & Disaster Recovery	**Q:** What business continuity and disaster recovery practices are established by Stratasys regarding health of vital services, data backups and restoration practices?	**A:** SWBU has defined and maintains a business continuity plan to ensure the highest level of service for customer issues or new product deliveries. All critical services are maintained at AWS to enable business continuity during disaster. The team maintains regular backups in the cloud. Maximum data loss never lasts more than 5 minutes. The team also runs annual disaster recovery tests as part of our SOP guidelines.
Security Incident Management	**Q:** Are customers contacted regarding Security Incidents in a timely manner?	**A:** SWBU maintains a comprehensive, step-by-step Incident Response Plan (“IRP”) to respond, resolve, and recover from a cyber incident. Customer and stakeholder communication plans are based on established protocols and activated, as necessary. However, security incidents regarding customers and their data have not occured in the past 5 years.

Commonly Asked Security Questions (FAQ)

Network Security	**Q:** Are all unnecessary network access points, ports, untrusted devices and protocols removed / disabled?	**A:** Yes. Employee and Guest networks are set up separately with no crossover. VPN and access to the network is limited to authorized users as per our SOP. Firewall and routers are configured to allow traffic from only trusted networks. Any devices accessing the corporate employee network are first approved by Stratasys IT teams.
Cloud Security (Only applicable when using Cloud Services)	**Q:** What cloud security policies are established to ensure secure handling and storage of customer data?	**A:** SWBU maintains a cloud security policy based on current industry standards for cloud security. A multi-tenant cloud infrastructure is implemented to ensure that each customer's data is logically segregated from others. Data access is granted selectively by internal admins and encryption keys are provided by trusted providers.

Disclaimers, Advisories and Resources

At Stratasys, everyone is involved and contributing to addressing the cybersecurity challenge. Stratasys knows that its customers are equally concerned and anticipate stringent and proactive measures to be implemented to stay safe.

For details on policies and legal aspects of operations, a GrabCAD terms of service statement and a statement from Stratasys is available. GrabCAD community's privacy statement is also relevant.

A wealth of best practices, frameworks and other information potentially of interest to customers are also worth consulting at the NIST web site.

For more information or to address any specific concerns you may have, please contact security@grabcad.com

GrabCAD Headquarters
Boston, MA
9 Camp St 2nd Floor,
Cambridge, MA 02140
+1 617 825 0313 (US Toll Free)

Minneapolis, MN
7665 Commerce Way
Eden Prairie, MN 55344

Israel
2 Holtzman St.,
Science Park,
Rehovot 76124