Procore Cloud Security Guide

An Overview of Procore's Security Measures

Table of Contents

How does Procore help Builders?

Builders worldwide are looking for ways to streamline communication and workflows, enabling collaboration across the entire project lifecycle. The competitive landscape and macroeconomic environment necessitate eliminating delays, increasing efficiency and productivity. Businesses are looking for ways to leverage best practices while creating their own differential advantage in how they work.

To that end, Procore provides construction management software that connects the entire project team, from the office to the site and across companies, providing one place to work together to do what they do best—build.

Using Procore, builders can more effectively deploy their information technology (IT) resources to value-added development, such as leveraging data insights. At the same time, Procore provides a scalable, flexible foundation. Procore provides enterprise-grade security and invests significantly in research and development. Software as a service (SaaS) users can enjoy significant operational and cost savings by leveraging economies of scale from their provider compared to building and maintaining an in-house solution.

In order to expand our platform, we offer open APIs that allow other applications to integrate, giving users the option to choose the tools that work best for them and their business. The platform is adaptable to unique business needs and processes today and tomorrow and supports the entire project lifecycle with an integrated set of applications.

Our platform provides access to a single source of data, reducing miscommunication, errors and rework; eliminating delays; and maintaining history

for future projects and dispute resolution, with a real-time, consolidated view of the entire project - so users know if projects are on-time, on-budget, and course correct quickly.

Procore streamlines communication and workflow enabling collaboration across the entire project team, eliminating delays, increasing efficiency and productivity. In addition, users have access to analytics in order to make sense of their data, gain a deep understanding of their business and improve decision making.

What does Procore do?

Procore manages your projects, resources and financials from project planning to close out. Our platform connects every project contributor to solutions we've built specifically for this industry - for the owner, for the HC and for the speciality contractor.

Procore is offered as a multi-tenant, Software as a Service (SaaS), cloud-based solution, and is accessed via the public internet (over a securely encrypted connection). With cloud-based technology, software and hardware management and maintenance tasks are offloaded to the service provider, which frees up resources for you to focus on driving value with your business. Procore is hosted on AWS Global Infrastructure and offers native mobile apps for iOS and Android.

Procore eliminates application silos, reduces double data entry, and keeps everyone on the same page with one source of up-to-date accurate data. Our App

Marketplace has nearly 350 partner solutions that integrate seamlessly with our platform, giving you the freedom to connect with what works best for you, even if we don't build it. It's how Procore gives your team access to everything they need to know to get their job done.

Procore Platform: Designed for Scalable Collaboration

What does Procore being a cloud-based SaaS solution mean?

Before Procore, users typically installed software on their computer hard drives, which ran a program. And they stored the data locally, on their hard drives. Later, software was installed on servers that resided at the customer's business so that people that worked in that office could access the program and store their information in-house. The challenges that companies faced with these approaches were:

1. Keeping software up to date
2. Maintaining enough storage space
3. Troubleshooting and repair
4. Ensuring access to information

Cloud-based solutions, like Procore, address all of these challenges.

Procore offers a cloud-based solution made available to customers as Software as a Service (SaaS). Data is securely stored for efficiency and accessibility for users. The service is delivered over the internet and accessed via a web browser or Android or iOS mobile application. This eliminates the need for a large capital expense to buy hardware and software to set up and run an on-site data centre.

+ The Procore team keeps the software up to date and secure, regularly introduces new functionality, and lets customers know when mobile updates are available. And we do this painlessly, much like how consumer apps are always improving at a rapid pace of innovation.
+ Procore makes unlimited storage available for an unlimited number of users. It is flexible to meet customer needs.
+ Procore offers 24/7 support to everyone on your team, including your collaborators. The average support response time to a user support request via online chat or phone in 2020 was under 60 seconds.

+ Procore has comprehensive security and logging tools for managing access and determining who can see what information, according to their role.

Procore offers a cloud-based solution made available to customers as Software as a Service (SaaS). Data is securely stored for efficiency and accessibility for users. The service is delivered over the internet and accessed via a web browser or Android or iOS mobile application. This eliminates the need for a large capital expense to buy hardware and software to set up and run an on-site data centre.

An added benefit of cloud computing is that data is backed up in multiple regional locations. This makes it easier to recover in the case of a disaster and supports business continuity. The storage is flexible and scalable, and the software is maintained remotely by Procore. Therefore, you can focus on building while we focus on building software for people like you, who build the world.

What does Procore being a platform mean?

Procore's software has a platform architecture, which means that each module you use connects to the others to make your project management process more efficient. There are a number of controls in place for communication, including built-in workflow mechanisms and permissions. For example, a Super or site foreman on a jobsite can entertime cards in Procore's mobile app. Team members can automatically see that information on the desktop application in the office. The information automatically updates the budget, timesheet reporting, site diary, analytics, and more.

When submittals are entered, the work plan and any related drawings automatically update, so everyone works off the latest information. Furthermore, when you upload your documents to Procore, they become dynamic and interactive through hyperlinks and markups. All of this is possible because of the way the system is structured.

Project Management is at the heart of Procore's solution which operates at job and portfolio levels. From there, our users extend the capabilities depending on their needs without reinstalling the software. This makes it possible for people across your organisation to access a single source of information, so everyone stays on the same page. Procore provides a unified experience as users go from one tool to another, making learning easier and more user-friendly.

Extensibility: Can I use other software tools alongside Procore?

Procore understands that users sometimes need specialised functionality that may only be available through third-party vendors. We designed the system with a set of tools that other vendors can use to connect to Procore. When you sign up for their services and provide them access, data can flow one-way or two-way between Procore and the third-party software. We maintain a list of over 300 partners in the API marketplace on our website.

Some of our customers have their own developers that want to develop applications. Or they want to build a connector to a third-party software. For this reason, we have an API developer toolkit. For more information on the integration process, please see the section below.

We hold ourselves and our partners to the highest standards.

Procore understands that there's a lot of trust on behalf of our customers to keep their data on the Cloud. Security is a top priority for Procore, and we continue to invest significantly in broad initiatives to ensure that our customers' data is safe, secure, and private. Procore uses a shared responsibility model which means that while Procore employees perform some administrative tasks, customers manage their accounts, data, projects, and more.

Who handles information security at Procore?

Procore's Information Security Team deploys a robust Information Security Program designed to address the processing of customer data, including transmission, storage, and access.

The Procore Information Security Team consists of the Procore Information Technology Team working alongside Product and Technology Security Engineers, Site Reliability Engineers, and Procore employees trained to minimise risk and protect data. Procore employees conduct all software maintenance and configuration activities for Procore's software and infrastructure.

Procore also engages third parties to review our program through an exercise called Penetration and Vulnerability Testing and auditing and ensuring compliance with a number of industry standards.

How is Procore's platform built?

Procore's platform is a fully cloud-native software as a service ("SaaS") solution. Procore is a multi-tenant solution with strong logical access controls using authentication and roles to ensure the necessary separation between data from client to client. All infrastructure responsibilities lay with Procore, and clients are provided with functionality to manage their own users and roles at the application level.

Procore is committed to protecting its clients, subscribers, employees, and Procore from damaging acts. Effective security and reliability is a team effort involving the participation and support of every Procore user who interacts with data and information systems.

What industry standards does Procore adhere to?

Our policies are designed to comply with all applicable laws, rules, and regulations. They are reviewed and updated regularly to remain compliant with the law and current industry practices.

Procore has documented and implemented policies and procedures based on the

National Institute of Standards and Technology (NIST) Cybersecurity and Risk Management Frameworks. This commitment to security as a continuous improvement process is important as new threats arise and existing threats evolve.

Procore maintains several certifications that recognise the controls we have in place to maintain security. These include:

IT security management standards:

+ (ISO) 27001:2013 Framework for confidentiality, integrity, and availability of information as well as legal compliance.
+ SSAE18 SOC. 2 How we maintain security and confidentiality

How does Procore design security?

Procore takes steps to protect your information throughout the Software Development Lifecycle and in the design of our architecture and infrastructure. Our Information Security team is consulted at each phase of development, and they are part of code reviews.

Where is customer information stored?

To provide redundancy and reduce latency, Procore uses a robust global network of servers in 15 locations, maintained by Amazon Web Services, for file storage.

All systems run monitoring tools with automated alerts integrated with an on-call rotation and automatic escalation. Information on which File Storage Profile is being used to house a customer's data is available in their portal.

- **Data Redundancy** means the same piece of information exists in multiple places. Having redundancy helps Procore restore the data in case of corruption or accidental deletion in the event of an incident.
- **Latency** refers to the time it takes for data to be transferred between its original source and its destination. By having a worldwide network of servers, customer data can be stored at a site in their designated region.

AWS provides enterprise-class tools that have been proven to be both reliable and secure for today's web-based applications. Amazon's cloud computing services are in use at companies of all sizes, from startups to large enterprises. By leveraging the AWS network, Procore can offer our customers unlimited data storage on the Procore Platform.

Data Centre Security and Compliance: How does Procore's Cloud Service Provider (CSP) safeguard data?

Amazon Web Services (AWS) is Procore's Infrastructure as a Service (IaaS) provider. AWS provides Procore and our customers the flexibility to scale as needed, and the knowledge that all data is hosted securely and privately. AWS provides the physical security access controls to the physical hardware used to provide the Procore solution. For more information on AWS security protocols, please refer to their webpage.

How does Procore monitor its data server provider?

Procore's relationship with AWS is as an Infrastructure as a Service (IaaS) vendor. They provide the hosting capacity on which we build the Procore SaaS platform.

AWS is not engaged in a consulting or product-specific capacity. They have no responsibilities or duties which are derived from the specific nature of our software or our customers.

The access granted to Infrastructure Partners is managed via technical controls based on the policy of least privilege as described in the Procore Information Security Handbook Vendor Management Policy:

“Access to Information: The provider must be given the least amount of network, system, and/or data access required to perform the contracted services. This access must follow applicable policies and be periodically audited.”

Procore Platform Access and Information Sharing

Procore takes steps to ensure the right people have access to the right information and the wrong people don’t. We built in tools and control mechanisms at multiple levels to help you collaborate and securely share information to the extent you decide.

RBAC and SSO: How does Procore handle access for users?

During the implementation process, company-wide settings are applied for access levels and security settings. These are called role-based access controls (RBAC). Administrators then execute these controls on an ongoing basis. For subsequent configuration changes, people with the appropriate permissions submit requests.

Procore provides a permissions template for administrators to expedite the process of designating permissions with the company and among external team members. Alternatively, this can be done manually. Administrators can also set up distribution groups. Procore provides options for role-based permissions for web and mobile applications.

Among the security setting selections are: lockout after failed sign-in attempts, password expiration, and idle session timeouts. Company administrators can unlock accounts.

Procore integrates with several popular single sign-on (SSO) providers, enabling users to use the same login credentials for other company applications. SSO is a user authentication process that gives users the ability to access multiple software applications using a single set of login credentials (i.e., an email address and password). If your company chooses to integrate an SSO solution with Procore, your end-users will sign into a central identity provider in order to access the Procore web application.

Who on my team can access specific information?

Procore is designed for collaboration across the entire project team. The Procore account holder, whether Owner, Head Contractor, or Speciality Contractor, determines which of their team members can access what category of information. This helps them strike the right balance between sharing information for greater efficiency and keeping proprietary information private.

In many cases, team members choose to have their own Procore instances, apart from the one provided by the principal account holder. This enables them to access the full set of Procore tools for internal record keeping and more efficient project management. For example, in the case of a speciality contractor, they can keep their own site diaries, record working hours, and more. For more information, please speak with your account manager.

A company or individual must be added to the Project Directory in order to see and access the project in Procore. This means, for example, that the administrator can set the permission level on Budgets to “none” for external parties. A “read-only” level access can be used in cases where a user needs to see information but does not have permission to change it. For example, a Super

needs to see commitments but does not change them. “Standard” access is used in cases where a user needs to interact with a workflow but would not be able to change it. An example would be writing or responding to an RFI. The “admin” level user can control the workflow.

Some Procore tools have more granular permission levels available to support additional use cases. For more information on permission levels, please see our support page on the topic.

Which teams at Procore can access my information?

Procore’s Access Control Policy adheres to the principle of least privilege, where employees, contractors, and all third-party vendors will be provided the least amount of access required to perform their job functions. Management is committed to testing and monitoring programs designed to ascertain whether the systems of controls and their component parts are functioning as intended and whether they afford an acceptable level of protection as time and technology advance. At a minimum, management will review access granting and control effectiveness on a semi-annual basis.

Direct access to client data is limited to legitimate business needs, including activities required to support clients’ use of the Procore SaaS applications. Employees may only access resources relevant to their work duties.

How can I share and distribute reports generated in Procore?

Procore customers benefit from having all of their project data in a single platform. That makes it available for reporting and analysis. Users determine how and when to distribute that information to their stakeholders, such as a periodic email to a distribution list. In some cases, they choose to post reports to third-party workplace locations such as Sharepoint. Procore offers options for integration so

that team members can consume the information in the location that best fits customer needs.

Network Security Management

Procore takes network security very seriously to ensure that customer data is transferred to and from the production system securely. Procore manages this through network observability, web application firewalls, hardened server configurations, patching, strong encryption, and DDoS protection.

How does Procore monitor anomalous network traffic?

Procore leverages a robust suite of observability and endpoint products to detect anomalous access patterns across the host, network, application, and DNS flows. If any anomalous events are detected, automations will kick off an incident according to industry-leading DEVOPS practices.

How are Procore's firewalls configured?

Following the principle of network segmentation, Procore only allows necessary communication for valid business purposes. System firewalls, network security groups and advanced WAF technology are employed to protect Procore assets. All system firewall rules are managed by configuration software and all changes are reviewed before deployment.

How does Procore protect against distributed denial of service (DDoS) attacks?

Procore utilises DDoS mitigation services from their hosting provider to protect all Procore production networks. These are robust cloud-based solutions encompassing real-time traffic modelling right down to server-level anomaly detection and attack mitigation and includes three layers of protection to identify and filter hostile traffic 24×7×365 to ensure customer uptime in the event of a DDoS attack.

How does Procore monitor for technical vulnerability and viruses?

Procore subscribes to manufacturer and independent security notification services to monitor potential external threats. The Product Security team works closely with Procore's Site Reliability Engineers (SREs) to ensure Procore assets remain configured to build standards. Procore's SREs use automated tools and documented procedures to build and configure all network equipment, systems, and servers from approved playbooks. Systems, platforms, and applications are configured to minimise security risks.

Leveraging state-of-the-art CSPM and Vulnerability Management tools, Procore continuously monitors all environments for vulnerabilities and risky misconfigurations. Our Vulnerability Management Program (VMP) handles identified vulnerabilities and misconfigurations. System patches are measured against documented Service Level Objectives (SLOs).

Procore has established a standard Incident Response Plan that is used for any application level or security incident. This is based on industry best practices and is reviewed regularly.

How does Procore secure applications?

Procore customers access the Procore environment via the public Internet. Transport Layer Security (TLS) is an encryption technology that Procore utilises to protect clients' private information while it is in transit via the Internet.

To protect all data stored by our customers on the Procore Platform, Procore encrypts that data while stored at our data centre providers.

Data at Rest (DAR): For DAR Procore utilises provider-managed device encryption services. This includes:

- AWS S3 Server-Side Encryption for all data objects
- Amazon EC2 EBS Encryption Full Disk Encryption for EBS volumes.

Data in Transit: Procore connections are secured using HTTPS protected by Transport Layer Security (TLS). The data in transit is encrypted using the AES256 standard, the secure hash algorithm (SHA-2) for message authentication, and RSA as the encryption key exchange mechanism.

All services use one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data. The provider-managed encryption services provide that the keys are securely managed.

Does Procore have a Bug Bounty Program?

Procore manages a Bug Bounty program that rewards security researchers that discover weaknesses in the security of the Procore platform. Discovered vulnerabilities feed into our Vulnerability Management Program (VMP) pipeline and are measured against documented service level objectives (SLO's) by severity.

How does Procore maintain data availability?

SYSTEM MONITORING, LOGGING AND ALERTING

Procore uses several industry standard enterprise application management solutions to monitor systems, trigger alerts based on event registers, and to facilitate alerting, trend analysis, and risk assessment.

Continuous monitoring of critical network events with our robust observability and eventing platforms give the Product Security team the ability to identify and address any unauthorised access to assets (including access to client data) within

the SaaS production network. Alerting is in place to notify the Product Security team of any issue.

DISASTER RECOVERY

Procore's disaster recovery (DR) plans and activities support the critical functions supporting the delivery of its SaaS application. Procore plans for the full spectrum of issues ranging from small-scale hardware failures all the way to widespread natural and manmade disasters.

Procore's disaster recovery approach is based upon system redundancy for our organisation's entire information technology infrastructure. The infrastructure is defined as all hardware and software used to deliver the Procore SaaS application. This redundancy extends to the diversification of hardware and software across geographical areas.

In addition to the application and data, Procore's application code (i.e., not including customer data) is kept in a secure online code repository. A commercial provider remotely hosts this repository.

Procore's customer data and assets are maintained in the application database and AWS' Simple Storage Service (S3). The database is remotely hosted by AWS Aurora and depends upon the Aurora High Availability and fault tolerance structure.

“Amazon Aurora automatically divides your database volume into 10GB segments spread across many disks. Each 10GB chunk of your database volume is replicated six ways, across three Availability Zones. Amazon Aurora is designed to transparently handle the loss of up to two copies of data without affecting database write availability and up to three copies without affecting read availability. Amazon Aurora storage is also self-healing. Data blocks and disks are continuously scanned for errors and repaired automatically.”

- https://aws.amazon.com/rds/aurora/faqs/#Backup_and_Restore

Additionally, Amazon Aurora Snapshots are used to ensure full availability of the database backup. A system-level failure, for any component in the Procore SaaS infrastructure, is easily identified and quickly resolved due to the hardware redundancy that is in place. All hardware is “hot-swappable” so that failed machines are replaced without bringing down the Procore application; the load balancers and firewalls in place are automatically swapped if issues are detected. Data centre redundancy is used to protect against natural and manmade disasters.

Procore’s hosting providers plan and construct their data centres specifically to withstand both natural and manmade disasters. For example, our data centre vendor equips its centres with on-site generators, diesel fuel storage tanks to power the generators, and multiple entry points for Internet backbone connections. Procore backups ensure that all project data is safely archived. Procore’s database is continuously copied to a secondary database, which is copied to a separate off-site data repository every 24 hours. All backups are written to RAID disk arrays in order to improve the reliability and availability of data and to ensure that data is not affected by hardware failure.

Should a disaster situation occur that renders the primary data centre completely unavailable, Procore has processes and procedures in place to restore access to the Procore SaaS application via a secondary data centre. The secondary data centre is physically located over 500 miles away and includes the same level of service, security, and infrastructure as the primary data centre.

SUPPORT AND INCIDENT MANAGEMENT

Procore has established a cross-organisation standard Incident Response Plan that is used for any application or availability incident. This is based on industry best practices and is reviewed regularly.

BACKUP AND RETENTION

Procore maintains a robust “high-availability” strategy to protect our customers against software problems, hardware failure, and large-scale natural disasters. The pillars of this approach are redundancy, geographic diversity, and replication of data. These pillars protect our entire information technology infrastructure. All hardware and software used to store customer data and deliver the Procore application to our customers is protected. Procore also maintains a disaster recovery plan in case a full restoration is needed.

Procore maintains several replicas of the application software on each server. This replication allows for fast roll-back in the event of a software issue. We maintain the software on multiple servers located in different secure data centres. This diversity protects against hardware failure and local service issues. In the event of any failure, our system logic sends any customer requests to another server. This redundancy allows us to service the affected system with no customer impact.

Our service providers host the database in secure data centres. Procore’s “simultaneous replication” architecture maintains the data across these data centres. Data is written to independent servers located in at least three separate locations at any time.

All data is copied to off-site storage every 20 minutes. Replication distributes this offline snapshot across the United States. Remote copies are maintained in secure data centres. These snapshots allow a complete recovery of the database as-of the snapshot time, protecting our customers against a region-wide disaster. The disaster recovery plan is designed to meet Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) to minimise any downtime or information loss for users.

Procore routinely tests and validates our ability to recover from a variety of problem scenarios. Our "test scenarios" range up to the scenario of total regional loss. Frequent testing ensures that our recovery plans allow us to meet or beat our aggressive recovery targets.

DATA EXPORTS

The Procore Extracts application is useful when your company wants to save an archive of a project's information. The application exports the data to a series of files and folders organised in a single folder on your computer. After the extraction process is complete, you can open the folder to view the data from the project by tool.

THINGS TO CONSIDER

Required User Permissions:

+ 'Admin' level permissions on the tools you want to extract data from.

Additional Information:

+ Important! For the extract to run and complete, there must be an active internet connection, and the computer must stay powered on. If you lose internet connection, or your computer goes to sleep or powers off, the system attempts to resume progress up to 3 times and then pauses the operation. Once the internet or power is restored, the extract automatically resumes.

- By default, the downloaded files from the extract are saved within an 'Extracts' folder on your computer. The Extracts folder contains a folder structure with the project name, the date and time of the extract, the project tools, and the items in the tools.
- Most items in Procore are downloaded as PDFs. Files such as documents and photos are downloaded as their original file type (for example, .xls and .jpeg).
- If the file path name was modified during the extract to save successfully, a “File Rename Information” CSV file appears in the folder. This file lists the original file name, along with the file name it was modified to.

Onboarding, Integrations, and Updates

What do onboarding processes and third-party application integrations look like?

IMPLEMENTATION

Procore's Customer Success team is dedicated to ensuring that you will have a successful rollout of Procore's construction management platform across your entire company and any new construction project. For larger implementation projects, a dedicated Procore Implementation Manager will walk you through each phase of the Implementation Roadmap. We also recommend that you establish an implementation team with focals for us to work with.

Ownership, Optimism, and Openness are Procore's core business values. We hope you join us in adopting these same values, especially during the rollout process. Together we will work as a team to ensure that the entire implementation process is both efficient and thorough. The goal is for each member of your team to be sufficiently trained on how to use Procore to perform their respective roles and responsibilities. Below is an overview of the implementation process. The details on each of the steps are available on our support website.

Partner Applications

Procore integrates with over 300 partner applications. For a full list of partner applications, please visit our app marketplace. We also offer a Procore Developer portal for custom connectors.

ERP Integration

A common integration request is for Procore to communicate with a customer's Enterprise Resource Planning (ERP) software. Considering Procore Platform's ability to manage project financials, integration with an ERP is a powerful combination. ERP integrations can be built by Procore, provided by a partner, or custom-built by either Procore or a third party. Procore has a growing list of available integrations.

In the case of SAP, which is a highly customisable solution, our team has a process for working with customers to ensure you maximise the value of your data and have a path to sharing information from the site to the front office to the back office.

While planning the ERP integration project, the customer team determines whether the data transfer will be one-way or two-way. A one-way data transfer, such as from SAP to Procore, reduces the project's complexity and provides utility while minimising any risk associated with data synchronisation. A two-way data transfer expands the utility of the data and may be part of the initial phase or a follow-up phase.

Procore works with customers to define integration points, so the data maps from our platform to the ERP system. We have a standard playbook to use as a

foundation. The linkages are between jobs, vendors, cost codes/work breakdown structures codes, budgets, contracts/variations, progress claims, payments, and more.

The customer IT department assesses the method of the file transfer. For newer software versions, and those with pre-built integrations, direct API calls will transfer the data. For older applications, flat files can be transferred via secure file transfer protocols (sFTP). In the latter case, an IT resource sets up the data transfer between the ERP system and the sFTP. Then Procore executes our standard sFTP to Procore chain. We would be happy to provide referrals to experienced integrators to set up the sFTP, if needed.

How does Procore manage software updates?

Procore regularly releases software updates with new features and improvements. We provide information and release notes on new releases, as well as early looks at upcoming new features. For more information, please see our Product Releases page.

The Procore SaaS solution is updated for all clients at the same time. There is no scheduled downtime window. Updates and Maintenance are designed not to affect the user experience. In the event that a planned maintenance issue would affect access to the platform, this would be communicated ahead of time so that any impact could be discussed with clients.

Procore's Product and Technology teams embrace an agile development & deployment framework. This allows individual product squads to continuously release fully Q/A'd product upgrades and enhancements across the entire platform, with the product releases happening multiple times per day/week.
For major functionality or UI updates, Procore will run a beta program and often allow for use of the "legacy solution" for a period of time to allow for testing and feedback.

Procore utilises Test and Development servers to provide testing and validation on any update to the platform prior to general release. For planning purposes, all releases, enhancements, and major changes are fully described and delivered to the system admin well in advance. Updates are communicated in several ways: In-app notifications, monthly newsletters, and monthly webinars.

Please take a moment to check out our Product Release Support page for further details.

Patches: Procore subscribes to manufacturers and independent security notification services to monitor potential external threats.

To ensure the system servers remain configured to build standards, Procore's SRE team uses automated tools and documented procedures to build and configure all network equipment, systems, and servers from predefined build configuration procedures. Systems, platforms, and applications are configured to minimise security risks.

Leveraging state of the art CSPM and Vulnerability Management tools, Procore continuously monitors all environments for vulnerabilities and risky misconfigurations. Our Vulnerability Management Program (VMP) handles identified vulnerabilities and misconfigurations. System patches are measured against documented Service Level Objectives (SLOs).

How does Procore enhance the software on an ongoing basis?

Regarding product enhancements, the most important thing about Product and Technology at Procore is the common thread of our customers. Nothing happens without the input, ideas, and consultation all coming from the customers.

There are a few ways that customers can get involved with Procore's Development Process. Anytime you think of something that Procore could be doing better or a problem that Procore is not solving, you can add it into the "post-an-idea" area in Procore. After doing so, you will be taken to our UserVoice Feedback Forum where you can vote on other users' ideas. This feedback informs our Product team's development priorities. We also run beta programs on new products and features and invite customers to participate.

Please take a moment to check out our Product Release Support page for further details. "For information on the international process for product release, please speak with your customer success manager."

In addition, Procore has established a community to ensure we are collecting the voice of the customer from everywhere, at every level. Procore wants to hear from our clients across all segments who are passionate about shaping the future of the construction industry, as well as Procore's products.

Procore User Groups are hyper-local, client-led meetings hosted by Procore users for Procore users. Expert users across the U.S. (and internationally) will plan and hold meetings, anywhere from quarterly to monthly, to discuss best practices, workflows, and tips and tricks around the Procore product and the industry as a whole.

Finally, several users have inquired about how they can find and connect with other Procore certified users. We've created a private group on LinkedIn in response to this request where any of the 40,000+ Procore certified users are invited to become members. See details here: https://support.procore.com/certification/tutorials/join-the-procore-certified-user-group-on-linkedin

Procore Resources

Procore Account Executives stay beside you to make sure the onboarding process goes smoothly. Our Customer Support team manages the integration process. Our technical services team gets engaged in executing the plan. We also provide on-demand and live training.

Procore will provide three key resources to our clients: an Account Executive (Sales), an Implementation Manager (Customer Success), and a Customer Success Manager (Customer Success).

Resources also include a variety of documentation, training materials, and services, such as an online support portal that contains written\tutorials, videos, FAQs, and guides, plus a hands-on certification program. Procore has materials to help a variety of learning styles.

Procore offers live training webinars with our dedicated customer success and support representatives. Classes are completely free and are offered every week. Each training session will also have some time reserved for live Q&A.

In addition to Implementation Managers, Customer Success Managers, and general support, Procore offers a group of Strategic Product Consultants (SPC) who are required to have an industry background and are partnered with specific product line development squads that align with their backgrounds. SPCs are

responsible for helping to educate our Customer Service teams, as well as consult our customers. Procore also offers specialised consulting services for a fee.