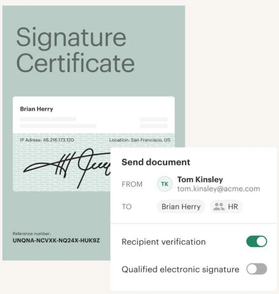
# Get enterprise-grade security for your most sensitive agreements

Our e-Signature software is compliant with E-SIGN, UETA, HIPAA, and GDPR. It's also backed by enterprise-grade security, so you can sign with total confidence.

Request a demo




### U.S. ESIGN Act and UETA

The U.S. Electronic Signatures in Global and National Commerce (ESIGN) Act and the Uniform Electronic Transactions Act (UETA) each require four conditions for a valid electronic signature: (a) intent to sign, (b) consent to do business electronically, (c) association of the signature with the record, and (d) retention of records. PandaDoc ensures compliance with these requirements under U.S. ESIGN and UETA laws.

### eIDAS and QES

The eIDAS Regulation 2014/910 establishes the legal framework for the three types of electronic signatures in the EU and the UK: simple electronic signatures, advanced electronic signatures (AES), and qualified electronic signatures (QES). QES is the highest standard, and PandaDoc provides QES-level signatures.

Learn more

### SOC 2 Type II

PandaDoc is SOC 2 Type II compliant. We can provide our latest SSAE 18 SOC 2 Type II report and attestation of compliance upon request.

Learn more

### GDPR

PandaDoc complies with GDPR by processing personal data lawfully, transparently, and only for specific legitimate purposes. We implement appropriate security safeguards, limit data collection to what is necessary, and uphold individuals' rights to access, correct, or delete their personal data.

Learn more

### CCPA

The California Consumer Privacy Act (CCPA) establishes consumer privacy rights for California residents and regulates businesses handling personal information. As the first U.S. consumer privacy law, it's comparable to the EU's GDPR. Effective January 1, 2020, the CCPA has been amended by the CPRA as of March 29, 2023. PandaDoc is CCPA compliant.

### Data Privacy Framework

The Data Privacy Framework (DPF) Program, created by the U.S., EU, UK, and Swiss authorities, allows U.S. organizations to securely transfer personal data from the EU, UK, and Switzerland while ensuring compliance with their laws. The EU confirms that the EU-U.S. DPF ensures adequate protection, enabling safe data flows. PandaDoc is a certified participant in the EU-U.S. DPF and its UK and Swiss extensions.

### HIPAA

PandaDoc is fully committed to helping healthcare providers protect patients' healthcare information when sending ePHI via PandaDoc. PandaDoc is compliant with HIPAA and the Privacy Rule, as well as the Administrative Safeguards, Physical Safeguards and Technical Safeguards of the Security Rule.

Learn more

### FERPA

PandaDoc helps schools facilitate electronic communication between educators, administrators, and school districts and parents and students in full compliance with FERPA (20 U.S.C. § 1232g; 34 CFR Part 99) as to protect the privacy of student education records.

### PCI-DSS

PandaDoc integrates with PCI-DSS compliant payment processors to offer payment processing via credit cards within the application.

### Data residency in US or EU

Choose where your data gets stored and processed. PandaDoc provides the flexibility your business needs to utilize these two equally secure locations.

Learn more

### Third-party Subprocessors

PandaDoc has agreements with all of its third-party subprocessors, used to provide various business functions, that require the subprocessor to meet PandaDoc's security and data processing standards.

Learn more

### 21 CFR Part 11

PandaDoc offers 21 CFR Part 11–compliant workspaces to help regulated industries meet FDA requirements for electronic records and electronic signatures. This includes enhanced signer verification methods, secure audit trails, and strict access controls, ensuring documents meet the standards for authenticity, integrity, and confidentiality.

Learn more

### FIPS 186-5 Digital Signature Standard (DSS)

PandaDoc uses FIPS-validated AWS CloudHSM cryptographic services for document signing. PandaDoc uses CloudHSM in FIPS mode, which is FIPS 140-3 certified and complies with the latest FIPS 186-5 Digital Signature Standard (DSS).

## Software security

### Servers and networking

All servers that run PandaDoc software in production are recent, continuously patched Linux systems. Additional hosted services that we utilize, such as Amazon RDS, S3 and others, are comprehensively hardened AWS infrastructure-as-a-service (IaaS) platforms.

### Storage

PandaDoc stores document data such as metadata, activity, original files, and customer's data in different locations while also compiling and generating documents when requested. All data in each location is encrypted at rest with AES-256 and sophisticated encryption keys management.

### Coding and testing practices

PandaDoc leverages industry standard programming techniques such as having a documented development and quality assurance processes, and also following guidelines such as the OWASP report, to ensure that the applications meet security standards.

### Employee access

We follow the principle of least privilege in how we write software, as well as the level of access. Employees are also instructed to use this principle when resolving customer support requests and when diagnosing possible software bugs that arise during development of new features.

### Isolated environments

The production network segments are logically isolated from other Corporate, QA, and Development segments.

### Customer payment information

PandaDoc uses external secure third party payment processing and does not process, store, or transmit any payment card data.

### System monitoring and alerting

At PandaDoc, the production application and underlying infrastructure components are monitored 24/7/365 days a year, by dedicated monitoring systems. Critical alerts generated by these systems are sent to 24/7/365 on-call DevOps team members and escalated appropriately to operations management.

### Service levels and backups

PandaDoc infrastructure utilizes many layered techniques for increasingly reliable uptime, including the use of auto-scaling, load balancing, task queues, and rolling deployments. We do full daily automated backups of our databases. All backups are encrypted.

### Vulnerability testing

Web application security is evaluated by the development team in sync with the application release cycle. This vulnerability testing includes the use of commonly known web application security toolkits and scanners to identify application vulnerabilities before they are released into production.

### Application architecture

The PandaDoc web application is multi-tiered into logical segments (front-end, mid-tier, and database), each independently separated from each other in a DMZ configuration. This guarantees maximum protection and independence between layers.

### Identity Verification

Add a robust layer of security to your documents with PandaDoc's Identity Verification options. Choose from four flexible methods: passcode verification, SMS verification, knowledge-based authentication (KBA), and ID Check. These options help ensure that only verified recipients can access sensitive information, supporting your compliance and security needs. Click here to learn more about PandaDoc's Identity Verification offerings.

### Secure and fair AI

We apply rigorous standards like secure data handling, encrypted processing, and protection against AI-specific threats, and work closely with our carefully chosen providers to protect your information. PandaDoc's systems are tested and monitored to ensure they're free from bias.