

Electronic Signatures: Security and Benefits **for Human Resources**

Quick, easy, and reliable e-signature app

ezsign

Table of Contents

4 **Introduction**

5 **How eZsign works**

6 **How you can use e-signatures**

7 **E-Signature benefits**

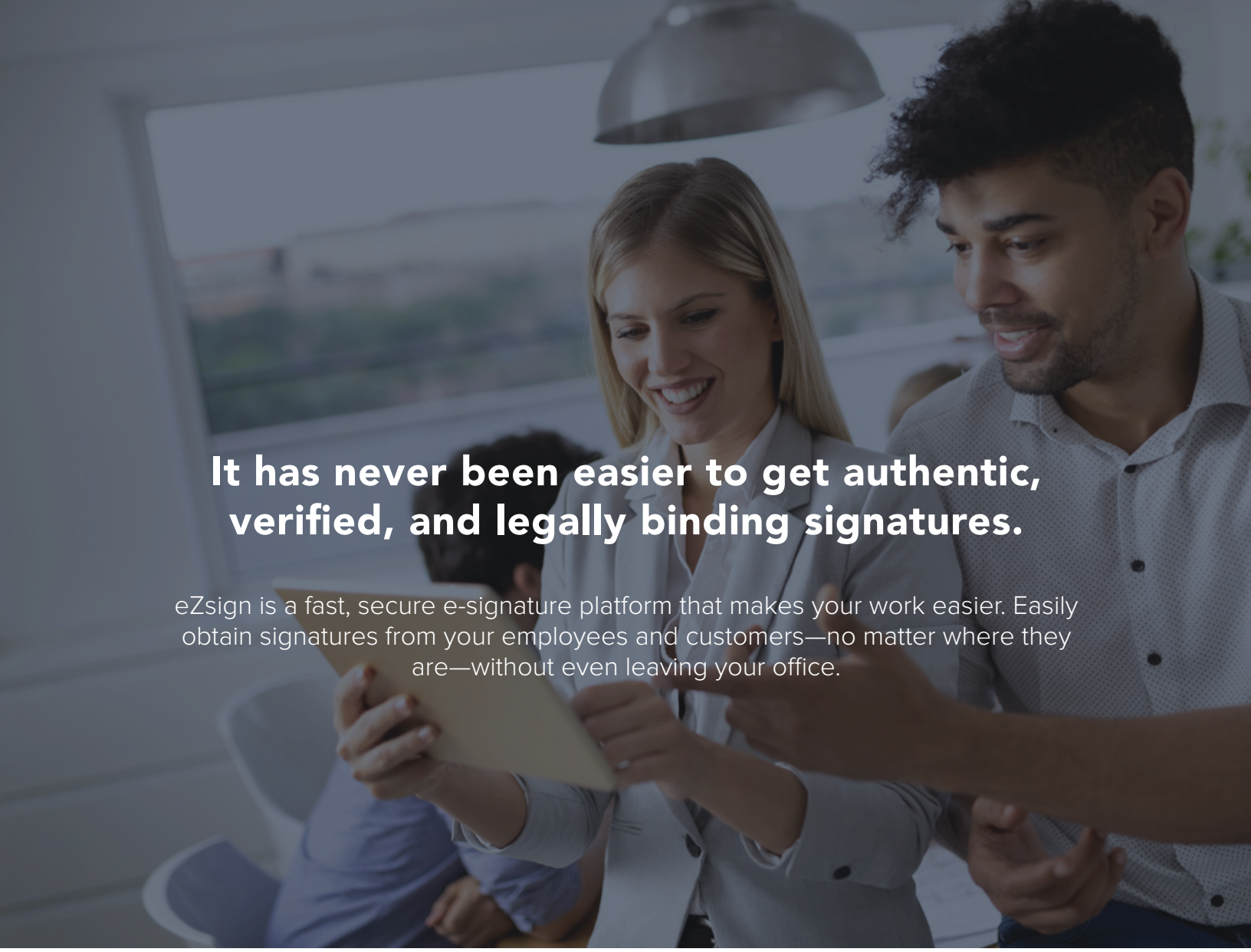
16 **Security Policy**

17 Security

21 Compliance

25 Confidentiality

26 Incident Response Plan



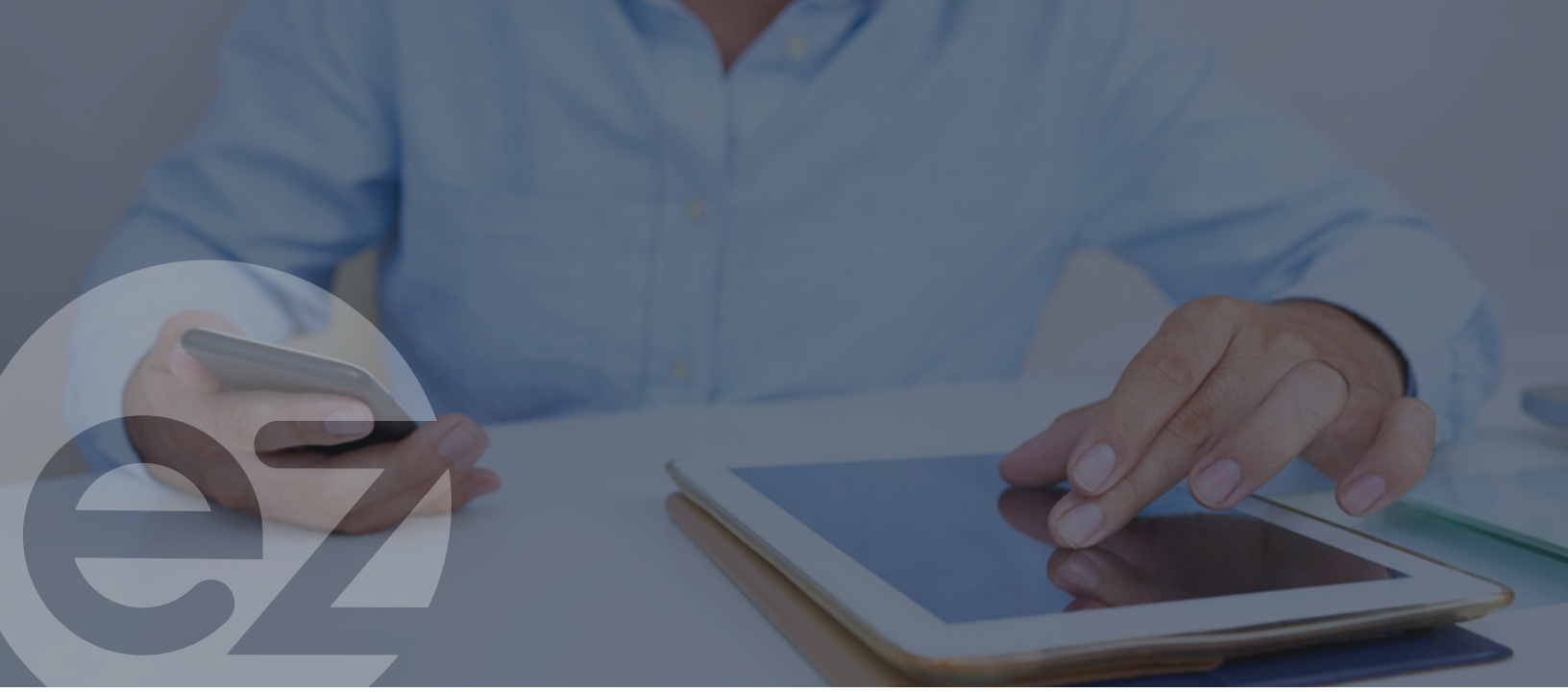
It has never been easier to get authentic, verified, and legally binding signatures.

eZsign is a fast, secure e-signature platform that makes your work easier. Easily obtain signatures from your employees and customers—no matter where they are—without even leaving your office.



A homegrown Canadian company

Buy local and fuel the Canadian economy



Our new normal: remote work

HR departments play a key role in important decision-making. Employee documents and physical personnel files create a mountain of paperwork that can be a real hassle.

In 2020, the day-to-day of thousands of businesses was turned upside-down seemingly overnight. This new reality forced many companies to find new tools to stay open, protect their employees, and serve their customers while staying safe.

2021 will be a year of recovery. The small businesses that modernize their workplaces and processes the fastest will be the ones that make a name for themselves.

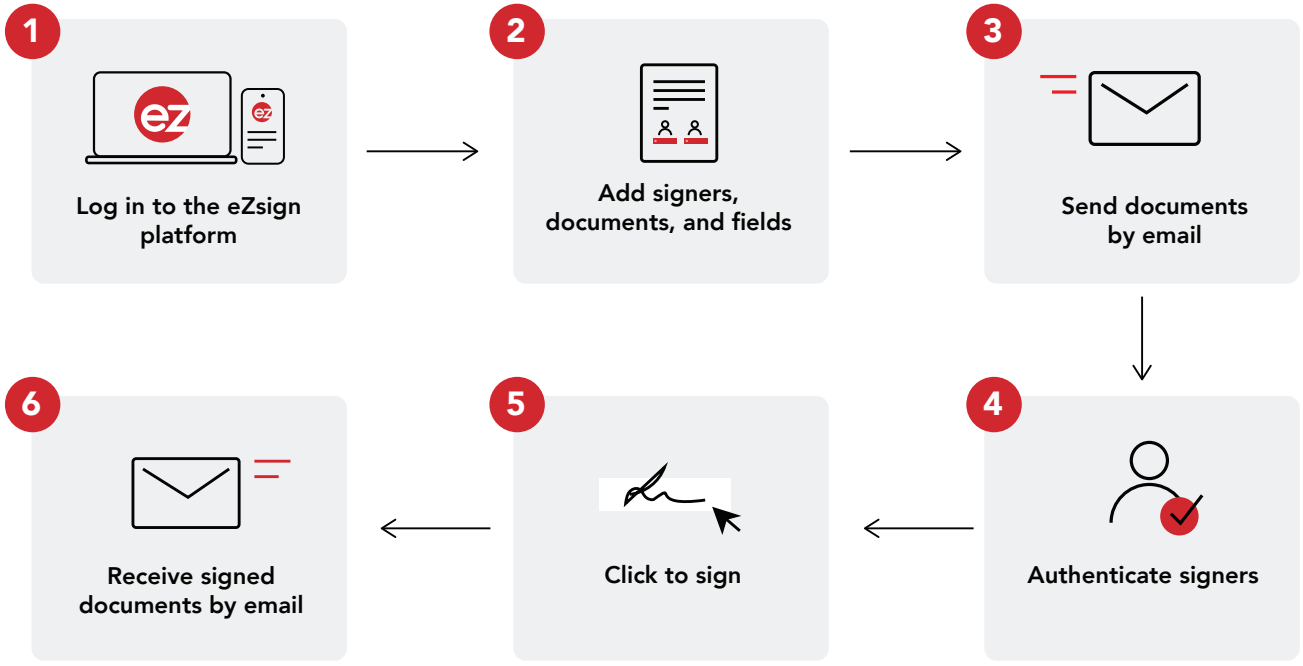
How can businesses make sure they keep operating smoothly now that brick-and-mortar offices as we knew them are a thing of the past? The solution: electronic signatures by eZsign.

E-signatures help you streamline your work and eliminate unnecessary paper pushing. Our outstanding security features set our solution apart. You can work with peace of mind knowing that your documents and data are completely secure.

This guide has three sections:

- How eZsign works
- Everything you need to know about the benefits of e-signatures
- Our commitment to security, compliance, and confidentiality

How eZsign works



Secure and trustworthy

Timestamping authority (TSA) for fraud prevention. Worry-free long-term validation (LTV) of signatures.

Signatures with just one click!

Employees and customers can sign documents on their computer, tablet, and even their smartphone.

Painless payment integration

Do you need to add a payment feature to your signing platform? We can help! Contact us for more information about processing payments easily and securely with Moneris.

ezsign.ca **1-844-EZSIGN2 (1-844-397-4462)**

Have you thought about all the ways you could leverage e-signatures?

Here are just a few of the documents you could be signing electronically:

Human resources:

- New hire forms
- Onboarding paperwork
- Employment agreements
- Codes of Ethics
- Internal policies
- Employee handbooks
- Performance evaluations
- PTO requests
- Expense account authorizations

Sales/procurement:

- Confirmation of receipt for bids and proposals
- Prototype, model, mock-up, and quote approvals
- Service agreements
- Purchase orders
- Order changes
- New customer forms
- New supplier forms
- NDAs

Are e-signatures legally binding?





Benefits of eZsign Electronic Signatures

Enhanced security

We take every possible measure to protect our users, their customers, and their documents against fraud and other security threats. Our e-signature security protocols rival those in place at many Fortune 500 companies.

Two-factor authentication

Two-factor authentication provides an added layer of security to ensure only the intended signer can access a document. eZsign features flexible two-factor authentication options, including receiving a text message or email or answering a security question. With this feature, users can rest assured only authorized parties are able to view and sign their documents.

Simplicity

Your customers will be pleasantly surprised by how easy eZsign is to use. Our simple and intuitive interface requires virtually no training to get users up and running. eZsign can meet even the most demanding customer requirements while still delivering an experience so user-friendly, anyone can learn to use it.

Increased efficiency

eZsign e-signatures can help you eliminate repetitive and redundant manual tasks and follow-ups to make your customers' and employees' lives easier. eZsign fits seamlessly into your workday and helps you streamline your processes. Reduce your admin time by up to 93% and improve your productivity by up to 80% by getting any document signed in minutes.

Easy and improved signature tracking

Ensure your administrative tasks stay on track. With our audit trail, you always know where your important documents are in the signing process. Set automatic reminders and receive notifications every step of the way. Once the eZsign process is complete, every party automatically receives a copy of the signed documents.

Unparalleled bilingual experience

Canada is a bilingual country, and eZsign is a fully bilingual application. We provide user support in both English and French and our library of online documentation and tutorials is also available in both languages.

With eZsign

49%

of documents are signed in

15 minutes

82%

are signed in less than

24 hours

Significant time savings

Time is money. On average, it takes seven days to gather signatures on paper documents. With eZsign, 49% of documents are signed in 15 minutes or less and 82% are signed in less than 24 hours.

eZsign allows you to standardize your processes for frequently used forms and documents, like contracts and agreements. Build customized templates with custom fields, recipient routing, and other settings that you can save and reuse.

Need to collect thousands of signatures for a document? With just a few clicks, you can send your documents to hundreds, if not thousands, of signers with eZsign's bulk and mass e-signature features.

eZsign also allows you to save and manage your contacts so you're never scrambling to find the right name, email address, or phone number. Fill out and save contact profiles for frequent signers and add them to a signing session with just a few clicks. This is perfect for approvals or contracts that require regular renewals.

Major cost savings

eZsign saves you money by reducing your fixed costs and improving employee productivity. With eZsign, you can reduce your direct costs related to printing, mailing, and storing paper documents—less paper, expensive ink and toner cartridges, stamps, and filing cabinets! With your employees working more efficiently, they have time for more productive tasks.

Fast adoption

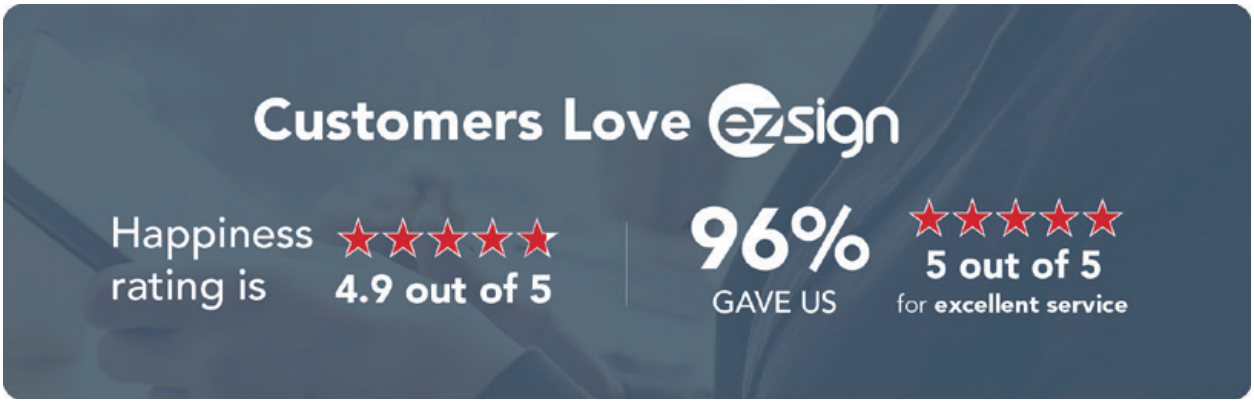
Training

Our eZsign training program includes courses and online tutorials to help your team get onboard with eZsign fast. We provide your administrators and users with the training they need to become eZsign experts in no time. Click here to learn about our training resources.

Unbeatable customer service

Customer service and customer experience are top priorities at eZsign. We assign every customer a dedicated Customer Success Manager, so you are always in touch with the same person if you have questions or concerns. Click here to learn more.

Plus, our customers love us! 96% of customers give us five out of five stars for customer service. We are proud of the service we provide, and we guarantee your satisfaction.



Seamless integration

Thanks to eZsign's simple e-signature API, you can easily integrate our solution into a variety of third-party applications you already use. For example, eZsign integrates with Moneris, Canada's most popular payment processor.

Scalability

Thanks to eZsign's cloud-based platform, you can scale eZsign e-signatures across your organization quickly and affordably. Configure your solution for as many signers, documents, and integrations as you need, and easily add or reduce the number of users.



Transparent pricing

eZsign offers transparent, cost-effective pricing to provide an economical solution that stays the same no matter how many documents you sign. Just one user? Our individual plan is perfect for you. Need to scale to the size of your team? We offer flexible subscriptions based on the number of users. View our pricing here or request a quote if you anticipate needing more than five users.

Improved accuracy

With an efficient e-signature platform like eZsign, you can reduce input errors by up to 18%.

Painless deployment

eZsign is cloud-based, so you can install it easily without needing an internal IT team or having to modify your existing IT infrastructure. Plus, you never have to worry about running updates. We handle everything for you.

Mobile compatibility

Our unbeatable cloud-based platform lets you work on the go. You can send documents from any computer or mobile device and users can sign from any internet-enabled mobile device.

Flexibility

eZsign offers a variety of settings and signing options to give you the flexibility you need. You can upload and customize your forms and signature fields, send and recall signature requests, set and extend signature deadlines, and more. With eZsign, you can send and sign legal documents securely from virtually any device.

Better collaboration

eZsign helps your teams work better together. Work with individual folders or use eZsign to create teams with shared folders for more effective collaboration.

In-person signing

Are you with the parties that need to sign your document and you don't want to wait to send them an email? No problem! The in-person signature feature lets you collect signatures right then and there on your own device.

Enhanced security and integrity

Working with eZsign means knowing you have a data partner who takes security seriously. We follow industry best practices for security and compliance, rivalling those of the world's largest companies and most trusted financial institutions. Our reputation—and our track record—speak for themselves.

Click here to visit our Trust Centre

User authentication

eZsign allows you to use or integrate with single sign-on (SSO) authentication protocols, such as LDAP and OAUTH. We also offer customization to incorporate other protocols as needed.

Timestamping Authority (TSA)

All eZsign signatures are TSA enabled, which means a trusted third-party timestamping authority provides a timestamp that ensures no party can falsify or forge the signature date or time. The timestamping authority acts as an impartial witness and proves exactly when documents are printed and signed.

Long-Term Validation (LTV)

All eZsign signatures feature long-term validation. This means that all signatures are protected and can be certified as legally valid by a third party for up to 25 years or more. Long-term validation acts like a digital notary journal to prove the validity of the signatures. Thanks to LTV, original signatures retain their validity, even if the document is re-signed or modified, and all document changes are logged.

Compliance at eZsign

At eZsign, we don't simply comply with industry standards and rules for e-signatures and cybersecurity, we go above and beyond to ensure the way we manage our network and keep data secure is always a step ahead. Learn how eZsign's unique features ensure our signatures comply with standards all over the world. Click here to go to the Compliance section in the Trust Centre on our website.

eZsign Availability

eZsign is powered by Amazon Web Services (AWS), the gold standard for secure, extensive, and reliable cloud infrastructure. With AWS as our cloud computing platform, you have access to your documents, even if there's a regional business disruption or data center failure. Click here to go to the Security (Cloud infrastructure) section in the Trust Centre on our website.

Confidentiality at eZsign

Privacy is paramount at eZsign, which is why keeping your data confidential is our top priority. We know that when our customers use eZsign, they are often communicating highly sensitive and confidential information, including personal information gathered and stored as part of their regular business operations. We recognize that it's our job to make sure your private information stays private. Click here to go to the Privacy section in the Trust Centre on our website.

eZsign SLA

With all the comprehensive measures we have put in place, our eZsign service-level agreement (SLA) promises 99.999999999% annual data durability and 99.99% application availability.

Legal and enforceable e-signatures

Our trusted combination of encryption, authentication, timestamping, and our industry-leading audit trail means that our e-signatures have the same legal validity as paper signatures, protecting your business in the event of a dispute. Click here to learn more.

Audit trails

Strengthen your compliance and avoid legal disputes with the most comprehensive audit trails on the market. eZsign saves all your signed documents and automatically generates and stores a robust audit trail for every file. Click here to read our FAQs.



“Thanks to eZsign’s robust security features, users can rest assured that signatures will stand up, even in a court of law—they are as valid as handwritten signatures”

– CLD Beauharnois–Salaberry



Security policy



Introduction

Security is a timeless business concern. In this digital age, information security has taken centre stage for all companies, including ours.

We know just how sensitive the business processes that involve electronic signatures are. Documents with electronic signatures often contain sensitive or confidential information, including personally identifiable information, trade secrets, commercial or financial information, medical information, and more. When it comes to handling and processing documents with e-signatures, security, compliance, and confidentiality are critical. Taking risks isn't an option.

As a software expert and trusted provider of software-based solutions since 2005, we understand the challenges companies face to ensure their infrastructure and data remain secure. Working with a reliable e-signature partner is essential. At eZsign, security is part of our DNA. It's an integral part of our business, which is why we've created this security policy. When you work with eZsign, you have the peace of mind that your data is in good hands with a partner that takes security seriously. We follow industry best practices for cybersecurity and compliance, rivalling those of the world's largest companies and most trusted financial institutions. Our reputation—and our track record—speak for themselves.

In the following sections, you can read more about how we've put security at the core of what we do, the regulations and standards we adhere to, the importance of privacy, and our response plan in the unlikely event of an incident:

Security
Compliance
Privacy
Incident Response Plan

Security

We are completely committed to ensuring that your documents and data are secure. From day one, we've designed and developed our eZsign solution with security as our top priority. We foster a culture of security in everything we do—from developing our software solutions to our day-to-day operations and customer service. This culture is reflected in four key overlapping areas: our management team, our employees, our processes, and our infrastructure.

Our management team

Our management team drafted this security policy to weave security in the very fabric of our company. To make sure we're following it, management also created a series of checks and audits to verify that we're complying with all its rules and procedures. Our management team is ultimately responsible for our information security and for the successful implementation of this policy. In addition to security, management is guided by a commitment to quality and to exceeding customer expectations. These practices aren't just good for our customers—they're also good for business.

Our primary goals in formulating and adopting this policy are as follows:

1. Create a system of rules to frame our IT security.
2. Ensure the behaviour of both individual employees and the company as a whole meets our expectations and complies with all applicable laws and regulations.
3. Ensure our systems, hardware, and resources are used appropriately so we can do business in a way that is consistent with our mission and that safeguards, showcases, and promotes our image and reputation on an ongoing basis.
4. Provide, foster, and maintain a safe, comfortable, and secure workplace environment where collective and individual rights are respected.
5. Encourage the people who fall under this policy to make positive contributions to the ways we envision, plan, and carry out our business activities.
6. Provide the people who fall under this policy with the resources and tools they need to effectively fulfill their roles, do their work, and assume their responsibilities.

Our employees

While our management team is ultimately responsible for eZsign security, everyone at eZsign plays an integral role. Every eZsign employee is tasked with ensuring that our data and that of our customers remains secure at all times. To that end, we perform a rigorous background check before every hire, and all eZsign employees follow a rigorous Security Code of Conduct and sign a confidentiality agreement before joining the company. We use access codes to restrict and monitor employee access to make sure our physical infrastructure and the data it contains are secure. All eZsign programmers and the entire IT team receive regular security training to ensure their knowledge of the latest trends in security technology is up to date and their skills are current. We also address security at every eZsign team meeting.

Every employee is responsible for promptly informing their direct supervisor if they find that sensitive information provided while using eZsign has been compromised or if they become aware of an incident or situation that could pose the risk of a security breach or affect the confidentiality of any sensitive information we are responsible for.

Our processes

We are committed to taking steps and implementing appropriate security measures to ensure we're able to protect the confidentiality, integrity, and accessibility of our customers' digital assets. To do this, we use industry-leading encryption for all documents and data that are sent or stored using eZsign. We have also developed access control and user authentication mechanisms as well as business continuity mechanisms in the event of an incident. These measures are proportional to how sensitive the data is, what it is used for, how much of it there is, and what format it is in.

Our processes must also be able to help prevent incidents and security breaches, errors, malicious acts, and the unauthorized disclosure or destruction of information. All our business processes include elements to this effect.

We have embedded security at every stage of the software development life cycle (SDLC) and regularly assess it to ensure our product is secure. We regularly conduct security tests in the following environments:

- Development (Dev)
- Quality Assurance (QA)
- Staging (Stage)
- Production (Prod)

Furthermore, we employ DevOps development practices such as continuous integration/ continuous delivery (CI/CD) and infrastructure as code (IaC) that allow us to monitor security at every step of the process. We have a dedicated security team that regularly audits information

security, physical security, and supplier risk both as part of and independent from the development process. These audits are performed at least twice per year.

We generate and store security activity reports and security event logs for all critical systems and data. We also track all eZsign-related activity, regardless of where this activity comes from, and generate and store relevant activity logs:

- Web activity
- Email activity
- File server activity
- Key management
- Virtual private network (VPN) activity
- eZsign application logins

Our infrastructure

Physical infrastructure security measures

The premises where eZsign data is stored are protected through 24/7 surveillance. The data is hosted in data centers having the certifications SOC 1, SOC 2, SOC 3 and ISO 27001. The entrances to the facilities are monitored and only those with permission can gain access.

We also use state-of-the-art applications and equipment to ensure that access to our development and production environments is restricted only to employees with proper authorization and training, which prevents access by unauthorized and/or malicious actors..

Data transmission and storage

We know your data is valuable, so we take every possible precaution to keep it safe. We use encryption standards that rival those used by the world's most respected banks and financial institutions to ensure that no one except you can access your confidential information. The eZsign application uses end-to-end encryption, which means we support the entire encryption chain from your device to our servers.

Safety mechanisms in place

1. HTTPS: TLS 1.2, RSA-AES128-GCM-SHA256, 128-bit keys
2. File storage and data servers (data at rest): AES256 encryption standard
3. Trusted timestamps issued by a trusted Timestamping Authority (TSA) per RFC 3161 timestamp protocol
4. OCSP servers integrated according to RFC 2560 and RFC 6960
5. FIPS 140-2-compliant hardware security module

Cloud infrastructure

eZsign relies on Amazon Web Services (AWS), the gold standard for secure, extensive, and reliable cloud infrastructure. With AWS as our cloud computing platform, you have access to your documents, even if there's a regional business disruption or data center failure.

- Highly available and redundant architecture that allows the entire system to withstand full site failure and always be running
- Multiple Availability Zones (AZs)
- Docker containers
- Real-time data replication
- DNS zones replicated across approximately 60 regions around the world (global DNS)
- Global content delivery network (CDN)
- Firewall and intrusion detection system (IDS) to prevent and detect attacks

With all the comprehensive measures we have put in place, our eZsign service-level agreement (SLA) promises 99.999999999% annual data durability and 99.99% application availability.

Compliance

Given how common electronic signatures are today and how important they are in transactions and business processes around the world, there is a patchwork of crucial regulations and standards to ensure global e-signature compliance. At eZsign, we don't simply comply with industry standards and rules for e-signatures and cybersecurity, we go above and beyond to ensure the way we manage our network and keep data secure is always a step ahead. We continuously monitor market intelligence to guarantee that our processes, systems, and approach remain compliant with the strictest international standards, especially as these standards change and evolve to account for new technological and business realities.

In addition to regularly auditing both virtual and physical risks, our dedicated security team also audits compliance with a range of international cybersecurity laws and standards. This active dedication to compliance with global laws, regulations, and standards allows us to ensure that the eZsign signatures on our customers' documents are enforceable and non-repudiable, no matter who signed them.

Below, we discuss the unique features of eZsign signatures that allow them to comply with standards all over the world.

Signature properties

- eZsign supports the latest digital signature technology standards, including PDF 2.0 in accordance with ISO 32000-2 and PAdES signatures, which are required by the European eIDAS regulation
- eZsign applies PDF signatures that can be validated using Adobe Reader, Adobe Acrobat, or any other validator that supports PDF signatures
- Validation information is stored directly in the signature per ISO 32000-1 or in a Document Security Store (DSS) as specified in ISO 32000-2 and PAdES part 4
- Signatures are applied in an incremental PDF update section to preserve existing signatures and document structure

eZsign supports all relevant PDF versions and standards:

- eZsign processes all PDF versions up to PDF 1.7 (ISO 32000-1), including extension level 8 and PDF 2.0 (ISO 32000-2)
- eZsign is aware of the PDF/A-1/2/3 (ISO 19005) archiving standards: if the input document conforms to PDF/A, the output document is guaranteed to conform as well. eZsign fully supports XMP extension schemas as required by PDF/A. The ability to insert PDF/A-conforming XMP metadata in PDF documents is an important advantage of eZsign

Signature characteristics

- E-signatures for Long-Term Validation (LTV) according to PDF 2.0 (ISO 32000-2)
- PAdES (ETSI TS 102 778 parts 2, 3, and 4, ETSI EN 319 142) and CAdES (ETSI TS 101 733) for qualified eIDAS signatures
- Signatures providing Long-Term Availability and Integrity of Validation Material (Level B-LTA) as required for eIDAS compliance
- eZsign retrieves a timestamp from a trusted Timestamping Authority (TSA) in accordance with RFC 3161, RFC 5816 and ETSI EN 319 422 and embeds it in the signature it generates
- eZsign creates document-level timestamp signatures per ISO 32000-2 and PAdES part 4

Cryptographic signature details

- RSA signature algorithm
- Strong signature and hash functions
- Full certificate chain embedded in the signatures generated, meaning signatures with certificates from a certificate authority (CA) on the Adobe Approved Trust List (AATL) can be validated in Adobe Acrobat and Adobe Reader without any configuration on the client side
- Embedded Online Certificate Status Protocol responses (OCSP according to RFC 2560 and RFC 6960) and Certificate Revocation Lists (CRL according to RFC 3280) as revocation information for Long-Term Validation (LTV)

Our solution also meets the following security and compliance requirements:

Electronic Signatures in Global and National Commerce Act (E-Sign Act)

The *Electronic Signatures in Global and National Commerce Act (E-Sign Act)* a U.S. federal law passed in 2000 that permits the use of electronic records and signatures for commercial transactions. It allows organizations to adopt a uniform e-signature process across all 50 states with the assurance that records cannot be refused by a court of law solely on the basis that they were signed electronically.

ISO 32000-2

The ISO 32000-2:2017 standard specifies a digital form for representing electronic documents to enable users to exchange and view electronic documents independent of the environment in which they were created or the environment in which they are viewed or printed.

ETSI TS 102 778-1

The ETSI TS 102 778-1 technical specification outlines the use of PDF signatures, as described in ISO 32000-1 and based on CMS, in any application areas where PDF is the appropriate format for the exchange of digital documents.

Uniform Electronic Transactions Act (UETA)

Like the *E-Sign Act, the Uniform Electronic Transactions Act* (UETA) is a U.S. law that was enacted to help ensure the validity of electronic contracts and the defensibility of electronic signatures. The UETA gives states a framework for determining the legality of an electronic signature in both commercial and government transactions.

Compliance with international, federal, and provincial laws

While third-party industry standards like SOC or ISO exist to certify entities' processes and are used to demonstrate compliance, there is no official certification per se for companies or customers to demonstrate compliance with international, federal, or provincial laws. Customers are responsible for ensuring that their data use complies with these laws, and our customers can rest assured that when they use eZsign, they are complying with all legal obligations under the following laws:

Personal Information Protection and Electronic Documents Act (PIPEDA)

A Canadian federal law to support and promote electronic commerce by protecting personal information that is collected, used, or disclosed in certain circumstances by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act, and the Statute Revision Act.

Freedom of Information and Protection of Privacy Act (FOIPPA)

An information rights law in the province of British Columbia that gives an individual a legal right of access to records held by provincial public bodies, subject to specific and limited exceptions. The act also requires that public bodies protect the privacy of an individual's personal information existing in records held by public bodies.

Personal Health Information Protection Act (PHIPA)

A law in the province of Ontario that sets out rules for the collection, use and disclosure of personal health information. These rules apply to all health information custodians operating within the province and to individuals and organizations that receive personal health information from health information custodians.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

A U.S. federal law that outlines the requirements for the management, storage, and transmission of protected health information in both physical and digital form.

Data centres

eZsign data is hosted in several Amazon Web Services data centres to provide our customers with superior access and availability. We work with AWS, an industry leader in cloud infrastructure solutions, because of their proven track record with compliance and the robust controls they have in place. Depending on your needs, we can guarantee that your data is stored on Canadian, American, and/or European soil.



See AWS certifications

Privacy

Privacy is paramount at eZsign, which is why keeping your data confidential is our top priority. We know that when our customers use eZsign, they are often communicating highly sensitive and confidential information, including personal information gathered and stored as part of their regular business operations. We recognize that it's our job to make sure your private information stays private.

We also recognize that the users or data owners under the *Act Respecting the Protection of Personal Information in the Private Sector* retain exclusive rights over their confidential information and may therefore request the materials that contain said information at any time. We know our users would suffer significant harm were this confidential information to be disclosed without authorization.

We therefore pledge to take all appropriate steps to keep all confidential information confidential:

1. We use industry best practices to ensure that user codes, passwords, and encryption keys remain confidential.

2. We make sure that anyone whose job involves handling or processing confidential information signs a confidentiality agreement. We also ensure they sign an agreement requiring them to comply with all relevant security measures to ensure that only they have access to the confidential information and limit the transfer or disclosure of such information. These agreements must be signed before they join the company.

3. We only use confidential information for the purposes for which it was supplied.

4. We work together with users and, if applicable, their end clients, to allow the intended persons to exercise their right to access, correct, or amend their personal information.

5. We work together with users to destroy personal information and user profiles in accordance with applicable retention schedules.

6. We cooperate with investigations and audits related to ensuring the confidentiality of personal or confidential information.

Incident Response Plan

Failing to plan is planning to fail. We go to great lengths to keep our IT infrastructure and our customers' data secure, but we also recognize that incidents can happen. We have therefore developed a detailed incident response plan in the unlikely event of a security breach. If an incident does occur, we will notify users within 24 hours if anyone has accessed or attempted to access their information without authorization, or if we discover a data breach or other incident that might affect data security or confidentiality.

Although eZsign has yet to experience a data breach, we recognize that every incident is unique. The end goal of an incident response plan is to protect our customers' data and ensure we comply with all legal and regulatory requirements. Below, you will find an outline of our current incident response plan, which has three steps: detection and analysis, containment and recovery, and improvement.

Detection and analysis

- Identify the incident or breach and verify whether it is ongoing. Before proceeding, ensure that any breach has been stopped.
- When an incident is reported, a qualified member of the on-call incident response team assesses the facts.
- Identify which parts of the system have been impacted and isolate them.
- Analyze all audit logs to determine whether data has been compromised, and if so, which data.
- If necessary, the team member launches the containment and recovery step.

Containment and recovery

- Focus efforts on finding the cause of the incident.
- Use audit logs to determine the scope of the incident.
- Take appropriate action to patch the entry point, remove the cause of the incident, and recover all systems.
- Work to limit the impact of the incident.

Improvement

- Analyze the incident to glean new information to improve tools and processes.
- Put necessary corrective measures in place.
- Document all changes and improvements.



ezsign.ca

1-844-EZSIGN2 (1-844-397-4462)

info@ezsign.ca