SECURITY POLICY

Security for your critical business data

This security policy document explains how we've considered your data security at every level in Everest Systems.

A MESSAGE FROM OUR CO-CEOS

At Everest, we understand that your business runs on trust.

When you choose our ERP platform, you aren’t just selecting software—you're entrusting us with your most critical business data, your operations, and ultimately, your company's future.

We recognize that you can only focus on growing your business, serving your customers, and achieving your goals if you have complete confidence in your technology partner. You should never lose sleep wondering if your data is secure, if your systems will be available, or if your information is protected.

That is why we apply our risk-based security approach to all our activities—so we stay on top of today's and tomorrow's security challenges.

Franz Faerber
Co-CEO
Everest
LinkedIn

Sandeep Chopra
Co-CEO
Everest
LinkedIn

Holger Mack
Security Lead
Everest
LinkedIn

What’s inside

Security at every layer

We know that an enterprise resource planning (ERP) software is home to your most critical business data, and we take our role and responsibility of protecting it seriously. Our executives have each spent decades in product leadership roles at the major ERP companies, and we know precisely what security you need at scale. That’s why we have built Everest the way we have. It is a unified platform on one unified data model with security considerations at every layer, from the beginning. We have implemented comprehensive measures in our software and operations to ensure the confidentiality, availability, integrity, and privacy of your information within all the systems you will build out.

We believe that a modern ERP with integrated security and compliance can free your team to be innovative and focus on business success. It is our ambition to give you enough trust in these systems that your teams can more confidently run a company that enters new markets, satisfies new regulatory requirements, launches new business models, and adapts with ease.

This Security Policy aims to demonstrate our dedication to earn and maintain your trust.

“We believe that a modern ERP with integrated security and compliance can free your team to be innovative”

You can trust our security around the globe

Our security commitment to you spans all Everest Systems entities worldwide, including our headquarters in Mountain View, California, our development center in Heidelberg, Germany, and our office in London, United Kingdom. We are accustomed to operating across continents and data privacy regimes.

Further, security is woven into every aspect of our operations. Every person in the Everest ecosystem, from full-time employees and contractors to third-party vendors, plays a vital role in maintaining our security standards. This extends down into the underlying infrastructure of our applications and the sensitive business data you depend on daily.

Our six security principles

1 Protect what matters most

We implement firm, risk-based defenses against unauthorized access through carefully designed access controls, system hardening, encryption, and monitoring.

2 Share responsibility

To achieve true end-to-end security, all participants (employees, customers, and partners) must work hand in hand under a clear shared responsibility model.

3 Your data should be available when you need it

We take strict measures to ensure our systems and your data remain available. We do this with redundant infrastructure, disaster recovery planning, and proactive monitoring that identifies and resolves issues before they impact you.

4 Continuous security

We've crafted our systems to ensure complete, accurate, and authorized data processing even in changing circumstances. We achieve this through rigorous security practices, controlled change management processes, and controls to prevent our systems and your data from unauthorized access to data or system disruption.

5 Security everywhere

We take a multi-layered approach to protecting sensitive information through data classification, strict need-to-know access principles, and comprehensive encryption and system/network hardening that protects data whether it's stored in our systems or traveling across insecure networks.

6 Compliance

We design our security and privacy approach in line with international standards, best-practices and regulatory requirements. This helps our customers trust that Everest is built to meet or exceed industry standards.

You can trust we'll never be idle

Security threats evolve constantly, and so do we. Our risk-based security approach recognizes that effective security requires continuous adaptation and improvement rather than static defenses. We continuously analyze and validate changes in our operating environment (e.g., customer requirements, changes in regulatory environment, or threat landscape) and if required, adapt our security and compliance approach to meet all expectations.

We integrate security into daily operations through policy-driven processes as well as integrated and automated controls that work behind the scenes. Our security leadership team, which includes our Co-CEOs and functional leaders from across the organization, regularly assess our security posture, make strategic decisions, and ensure our security investments align with business priorities.

This approach emphasizes transparency and shared responsibility. We maintain open communication about risks and mitigation strategies, which ensures rapid response to emerging threats. We empower every employee to contribute to our security posture by identifying improvements and concerns.

Five security controls you can rely on

1 Access management

Only authorized people can access the right resources at the right time. We use centralized authentication with multi-factor requirements, implement role-based access controls following the principle of least privilege, and conduct regular access reviews to maintain security as our organization evolves.

2 Comprehensive data protection

We treat all data according to its sensitivity level through our classification system spanning Public, Internal, and Confidential categories. We encrypt data both at rest and in transit and deploy comprehensive monitoring to prevent data loss while ensuring legitimate access remains seamless.

3 Robust infrastructure security

We use hardened cloud infrastructure with redundancy to ensure both security and availability. We maintain continuous vulnerability management with regular security patching, implement network segmentation, and deploy intrusion detection systems that provide early warning of potential threats.

4 Secure application development

Everest integrates security considerations from the earliest stages of our work through our secure development and operations lifecycle. We enforce that through regular code reviews, security testing, and vulnerability assessments. We regularly employ independent security experts and penetration testers to test and validate the security of our systems

5 Incident response

We combine security monitoring with well-defined incident response capabilities. Our escalation procedures and communication protocols ensure that any security events are addressed quickly and effectively, while regular testing and continuous improvement keep our response capabilities sharp.

Security is a shared effort

We work hand-in-hand with our customers on security and compliance. While customers have full control on who has access to their business data, Everest takes care to provide a secure and compliant platform and infrastructure you can trust.

Everest's integrated and risk-based security approach

Customer

You fully control who can access your ERP and data

Everest

Everest provides a trusted, secure, performant, reliable, and compliant platform

Everest ERP

Product features

- MFA and identity integration
- Audit log
- PII processing
- Integration configuration

Everest platform frameworks

- Authorization framework
- Audit log frameowrk
- Secure sandboxing
- Tenant isolation

Communications channel

- Security@everest-erp.com
- Slack channel
- Everest issue portal

Independent verification

- SOC2 Type II
- SOC1 Type II (planned)
- ISO 27001 - 2023
- Third-party penetration testing
- Contractural framwork
  - Master Services Agreement
  - Data Processing Agreement

Secure dev and ops lifeycycle

- Threat modeling and security reviews
- Security training
- Secure coding and peer review
- Automated testing
- Vulnerability management
- Penetration testing (internal, external)

Infrastructure and data security

- Incident response
- Access management
- Network islolation
- Multi-factor authentication (MFA)
- Security monitoring and threat detection
- Automated security scans
- Data at rest encryption
- Encryption over untrusted networks
- Backup and recovery
- Multi-availability zones

Platform providers

Leading cloud infrastructure providers and sub-processors

IaaS provider: Amazon Web Services

- Full sub-processor list: https://everest.systems.com/legal/sub-processors
- Third-party vendor management
- Secure AI/LLM framework usage

Our security is independently verified

We consider third-party verification an important cornerstone of the Everest security approach. It provides us and our customers with an independent, objective, expert assessment and confirmation that our approach is in full compliance with leading security standards.

For example, our SOC2 Type II attestation provides independent validation of our security, availability, and confidentiality controls and our commitment to information security management best practices. We maintain full compliance with data privacy regulations including GDPR, CCPA, and the UK Data Protection Act, ensuring our customers' privacy rights are protected regardless of jurisdiction.

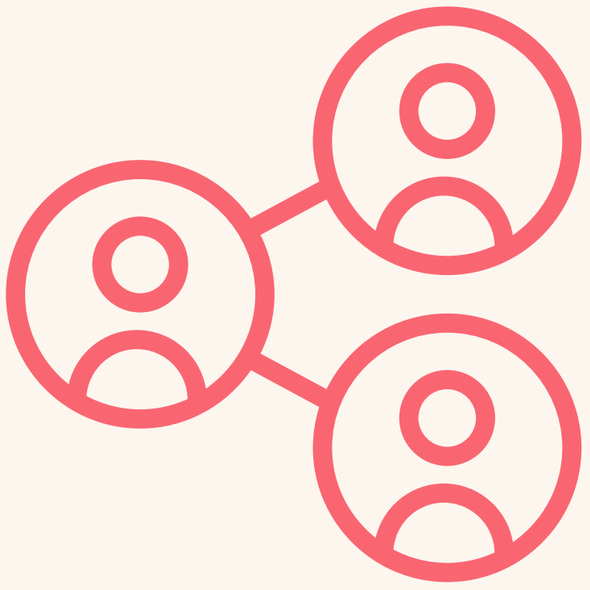
Independent third parties regularly assess our security program through compliance audits, penetration testing, and security reviews. These assessments provide objective validation of our security measures and identify opportunities for continuous improvement.

Accountability at every level

Security at Everest starts at the top and extends throughout our organization. Our Co-CEOs maintain ultimate accountability for our security program and regularly report to our Board of Directors on security status, investments, and risk management.

Our Chief Information Security Officer owns the day-to-day implementation and management of our security program, ensuring that our policies translate into effective operational practices that protect our customers and business.

However, security is everyone's responsibility. Every employee, contractor, and partner plays a crucial role in maintaining our security standards through their adherence to policies, participation in training programs, and proactive identification of security concerns.



SECURITY POLICY

We want to hear from you

We maintain open channels for security-related questions, concerns, and incident reporting because we believe that communication is essential to effective security.

For any security matters, you can reach us at security@everest-erp.com.

This Security Policy provides the strategic foundation for our comprehensive security program. Detailed procedures, technical standards, and implementation guides are maintained in our Security Handbook and supporting documentation, ensuring that our security commitments translate into effective day-to-day practices that protect our customers and business.

Version 2.0, 19th of March 2026
Document Classification: Public
Distribution: All Everest systems personnel and interested parties