Normative Security Whitepaper

Document Owner: Compliance

Introduction

To achieve Normative's mission to make known the sustainability impact of all economic activities on the planet, Normative must process all known economic activities. This data however is commercially and operationally sensitive to our partners and thus it is crucial for Normative to ensure the confidentiality, integrity and availability of Customer Data.

Normative takes great care to manage security, which is implemented through a shared security model in conjunction with a number of trusted sub-processors. Normative's ISMS has been externally certified against ISO 27001:2022. The sub-processors primarily includes Amazon Web Services (AWS), MongoDB Atlas, Auth0, SendGrid, Google Cloud Platform (GCP), Cloudflare & Luzmo (formally Cumul.io).

As an organization we fundamentally adhere to the ZeroTrust concept. Simply stated, the core tenet of ZeroTrust being: "never trust, always verify."

Infrastructure and Network Security

Physical Access Control

Normative servers and databases are hosted on Amazon Web Services (AWS) infrastructure within the EU. Amazon data-centers feature 24-hour manned security, biometric access control, video surveillance, and physical locks. All systems, networked devices, and circuits are constantly monitored.

AWS facilities are accredited under ISO 27001, SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II), PCI Level 1, FISMA Moderate and Sarbanes-Oxley (SOX). See AWS Security for more details.
Normative employees do not have physical access to AWS data centers, servers, network equipment, or storage.

Databases specifically are managed through the platform MongoDB Atlas which has been independently audited and confirmed to meet standards for data security accredited under SOC 2 Type II, ISO/IEC 27001, PCI DSS 3.2.1 and CSA STAR level 1.

Logical Access Control

Normative is the assigned administrator of its infrastructure on AWS directly while our databases are hosted on AWS but managed directly by MongoDB Inc. through the platform MongoDB Atlas. Only designated authorized Normative operations team members have access to configure the infrastructure on an as-needed basis behind a two-factor authenticated virtual private network.

Network Segmentation

Our production and development network is segmented into different zones. Each environment has its own subnet, and internal communications are only permitted based on a predefined allow list-based network policy.

Normative uses Twingate as a zero-trust access solution used to control access to individual resources in our AWS development and production environments. It enables fine-grained access control to individual resources instead of whole networks.

Twingate's client authenticates the user via SSO (inc. MFA) and, given the access configured for such a user, enables them to establish connections to such resources. It provides a split tunnel, so only the network traffic destined to the accessed resource is routed via this connection. A further benefit with Twingate is that the employee network itself can remain invisible to the Internet rather than exposing a public gateway to the Internet.

Penetration Testing

Every year Normative schedules penetration testing conducted by an independent, third-party agency. 2023's was in conjunction with Cobalt. For testing, Normative provides the agency with information about the internal network, including its documentation regarding its architecture and design, in addition to user and administrative accounts to access the system.
We permit customers to conduct penetration testing on our systems in certain circumstances. Customers must have prior approval from, and give advance notice to, our security team about the timing and scope of a penetration test and may be required to sign an agreement that covers such testing activities. Contact your account manager for more information.

In the case of any findings, mitigation and remediations are prioritized and actions against pre-defined KPIs.

Infrastructure Change Management

Each proposed change to our production environment (including infrastructure changes) must be peer reviewed and approved, and each such change and corresponding approval are logged. Our CI/CD pipeline provisions infrastructure changes in an automated manner after they are approved.

Secrets Management

Normative uses a secrets management system - AWS Systems Manager, to store secrets such as authentication tokens, passwords, API credentials and certificates. Keys are rotated on a regular schedule. All data is encrypted at rest and in transit.

Server Hardening

We use Amazon Web Services to provide pre-hardened server infrastructure. We interact with servers predominantly by deploying Docker containers using infrastructure-as-code orchestrated with AWS ECS.

Business Continuity and Disaster Recovery

Normative's platform has a documented RPO of <12 hours and a RTO of <24 hours. A number of controls are maintained towards this goal, including:

- Encrypted database backups (dumps and snapshots) generated at a frequency starting at hourly and stretching to monthly for up to three months. Backups are stored across multiple availability zones across multiple regions - Germany and Sweden, with strict technical controls on access and immutability.

- Automated integrity and restoration checks are run on a weekly basis and annual disaster recovery rehearsals are undertaken and documented.
- Quarterly business continuity tests are ran on supporting business processes.

Cryptography & Encryption

Encryption in transit

All data sent to or from our infrastructure is encrypted in transit via industry best-practices using Transport Layer Security (TLS 1.2+). Externally this is ensured by configuration in Cloudflare. A live report on the certificates can be generated here - https://www.ssllabs.com/ssltest/analyze.html?d=app.normative.io

Encryption at rest

All Customer Data is encrypted using the AES256 encryption algorithm in our databases and file stores. The data keys are themselves encrypted using a master key stored in a secure key store and rotated on a fixed schedule.

Application Security

Vendor Management

We work with vendors and service providers who help us to provide our services to customers, cloud hosting providers and cloud service providers. Vendors are chosen and implemented via a framework.

First, we select vendors based on our experiences working with them, their reputation, and an evaluation of how well they meet our requirements.

Secondly, we perform due diligence on potential vendors, which includes a risk assessment of their security posture & review and implementation of their CEUCs.

Thirdly, when we engage a new vendor, we ensure that we have a written agreement with them that includes appropriate provisions with respect to confidentiality, security, privacy, and service levels, where relevant. Vendors are only permitted to use data provided to them for the purpose of providing their services to Normative.

Third-Party Authentication Platform

Auth0 is used as an authentication platform to enable Single-sign on (SSO) for our users using Google or Microsoft, regular email and password sign-in plus TOTP-based MFA (which can be enforced tenant-wide). Auth0 further has a range of security safeguards to prevent user credentials from being leaked or an attacker successfully taking over a user's account. Examples are bot detection & prevention, brute force protection, breached credentials scans & suspicious IPs blocking from user context.

Auth0 further comes with a list of certifications including but not limited to: ISO 27001; ISO 27018; SOC 2 Type II & Gold CSA STAR level 2.

Application security monitoring

- Renovate is used for vulnerability management (and license management) of the OSS libraries included within the platform
- Detectify is used to perform weekly vulnerability scans.
- We use a security monitoring solution to get visibility into our application security, identify attacks and respond quickly to a data breach.
- We use technologies to monitor exceptions, logs and detect anomalies in our applications.
- We collect and store comprehensive logs to provide an audit trail of our applications activity. Our logs are frequently reviewed by our security team to identify anomalies.

Web Application Firewall (WAF)

We use a runtime protection system that identifies and blocks OWASP Top 10 and business logic attacks in real-time.

Email Security

The Normative service includes email notifications triggered by Auth0 sent via SendGrid (a Twilio company). SendGrid has a wide array of security measures and has undergone SOC 2 Type II attestation.

Sender policy framework (SPF) is a system to prevent email address spoofing and minimize inbound spam. We have SPF records set through Cloudflare, our domain name service (DNS), and domain-based message authentication, reporting, and conformance (DMARC) set up for monitoring reports to reduce the risk of phishing scams.

Secure Application Development (Software Development Lifecycle)

Normative practices continuous delivery, which means all code changes are committed, tested, shipped, and iterated on in a rapid sequence. A continuous delivery methodology, complemented by pull request, continuous integration (CI), and automated error tracking, significantly decreases the likelihood of a security issue and improves the response time to and the effective eradication of bugs and vulnerabilities.

Corporate Security

Information Security Management System (ISMS)

Normative runs a security program, scoped to its handling and processing of Customer Data, which is aligned to ISO 27001:2022.

It is overseen by Normative's Security Leadership Steering Group (SLSG), composed of the CEO, CTO, and COO, with annual reviews by the company board. Operationally it is managed by the Head of Compliance, acting as ISMSM, with involvement from stakeholders around the company.

Security Policies

Normative maintains an internal repository of security policies, which is updated on an ongoing basis and reviewed annually (plus ad hoc as necessary).

Acceptable Use Policy v1.4.1-2024-03-27
Asset Management Policy v1.0-2023-11-21
Backup Policy v1.1.2-2024-03-18
BIA Template v1.1.1-2023-09-11
Business Continuity Plan v1.0-2023-09-11
Code of Conduct v1.1.1-2024-03-18
Change Management Policy v1.0.1-2023-12-25
Data Classification Policy v3.5-2024-03-27
Data Protection Policy v1.2-2024-03-18
Data Retention Policy v4.3-2024-03-27
Disaster Recovery Plan v2.1.2-2024-01-28
DS student compliance process v1.1-2024-03-18
Encryption Policy v1.0-2023-12-25
End of life process v1.0-2023-08-29
Incident Response Plan v5.3-2024-03-27
Information Security Policy v3.2.2-2024-03-30
Internal Audit Plan v1.0-2024-02-12
LIA Template v1.0-2023-10-10
Password Policy v1.3-2024-03-23
Physical Security Policy v1-2023-12-27
Policy Template v1.1.1-2023-10-21
Remote Work Policy v1.0-2024-03-17
Responsible Disclosure Policy v1.1-2023-12-28
Risk Assessment Policy v1.1.1-2024-03-27
Software Development Life Cycle Policy v1.2-2024-03-27
Subject Access Request Process v1.1-2023-11-01
System Access Control Policy v1.3-2024-03-30
Vendor Security Management Policy v1.1-2024-02-15
Vulnerability Management Policy v2.0-2023-10-22

Audit Program

As part of the ISMS, an internal audit is performed once a year, covering all clauses of ISO 27001 and all implemented controls.

As of April 2024, Normative completed its external certification against ISO 27001:2022, the certificate for which can be found here.

People Security

Workforce Security Training

All new employees receive onboarding and systems training, including environment and permissions setup, formal software development training (if pertinent) and security policies review.

Additionally, employees receive periodic security refresher training and updates about security best practices. Employees are required to review and acknowledge that they have reviewed the company's information security policies and procedures, which include an acceptable use policy for IT resources.

All engineers further review security policies as part of onboarding and are encouraged to review and contribute to policies via internal documentation. Major updates are communicated via Slack to all Normative employees.

Device Security

Via MDM, all employee computers are centrally configured and monitored to have anti-virus/anti-malware software installed, full disk encryption, firewalls, network share restrictions & fixed period screensaver lockouts.

Physical Security

Normative has entities and offices in Sweden, Denmark and the UK with most workers operating in a hybrid fashion. Normative employees are instructed and trained to ensure that their physical working environment is kept secure (be it at the office or at home) and that any work equipment is secured appropriately, including when not in use.

Storage & deletion of Customer Data

Customer Data is only stored in the designated data stores - platform databases and buckets, with security enforced via IaC, except if manual review or troubleshooting is necessary. In such cases the data is always stored in an encrypted format and erased from the temporary location as soon as the work is completed.
Clause 7.3 of the General Terms makes reference to Normative's deletion processes, which by default are triggered within ninety days of the end of the agreement, or on instruction from a Customer administrator.

Employee Confidentiality Obligations

All employees and independent contractors are required to sign contracts under which they agree to protect customer and other proprietary information as confidential information. Our employee handbook and security training (onboarding + annual refreshers) stresses the importance of maintaining the confidentiality of customer data.

Offboarding Employees

We have documented processes that we follow to ensure that when an employee departs the company, their access is revoked in a timely manner (including specifically within one business day for all Customer Data systems, IdP/SSO and IT) and any company assets they possess are returned, securely wiped and asset tracked.

Incident process

Normative follows the incident handling and response process recommended by SANS, which includes identifying, containing, eradicating, recovering from, communicating, and documenting security events. Normative notifies customers of any relevant incidents without undue delay through the appropriate medium(s), followed by multiple periodic updates addressing progress and impact. Normative Enterprise plans include a dedicated customer success manager who holds responsibility for customer communication, as well as regular check-ins and escalations.

Normative maintains a live report of operational uptime and issues on our status page. Anyone can subscribe to updates via email, sms or Slack from the status page. Any known incidents are reported there.

Vulnerability Disclosures

Anyone can report a vulnerability or security concern with a Normative product by contacting through the details https://normative.io/.well-known/security.txt and including a proof of concept, a list of tools used (including versions), and the output of the tools. We take all disclosures very seriously, and once we receive a disclosure we rapidly verify each vulnerability before taking the necessary steps to fix it. Once verified, we periodically send status updates as problems are fixed.

Version History

Date	Version	Author	Notes
2021-10-28	1.0	Adam Wamai Egesa	First external release.
2022-02-10	2.0	Javier Martinez	Various updates.
2023-02-10	3.0	John Henry Mostyn	Annual review.
2023-06-12	3.1	John Henry Mostyn	Re-designed visuals. New reference to ISMS policy set, various details tweaked including details around Auth0, improved gray box pen test details, application security monitoring measures, an updated introduction and clarification on pen test cadence (every year).
2023-09-15	3.2	John Henry Mostyn	Updated details around key sub-processors & database backup procedures.
2023-12-04	3.3	John Henry Mostyn	Updated security vulnerability disclosure process, vulnerability management, added reference to the terms deletion clause, added penetration testing detail, minor branding tweaks.
2024-01-23	3.4	John Henry Mostyn	Removed reference to Aiven
2024-03-30	3.5	John Henry Mostyn	Updated ‘Security Policies’ section.
2024-04-24	3.6	John Henry Mostyn	Added ISO 27001 certification details. Refreshed policy table.
2024-07-24	3.7	John Henry Mostyn	Added additional detail on existing Disaster Recovery controls.