23

TwentyThree Security Policy and Practises

Version November 2021

For an updated version refer to
https://www.twentythree.com/policies

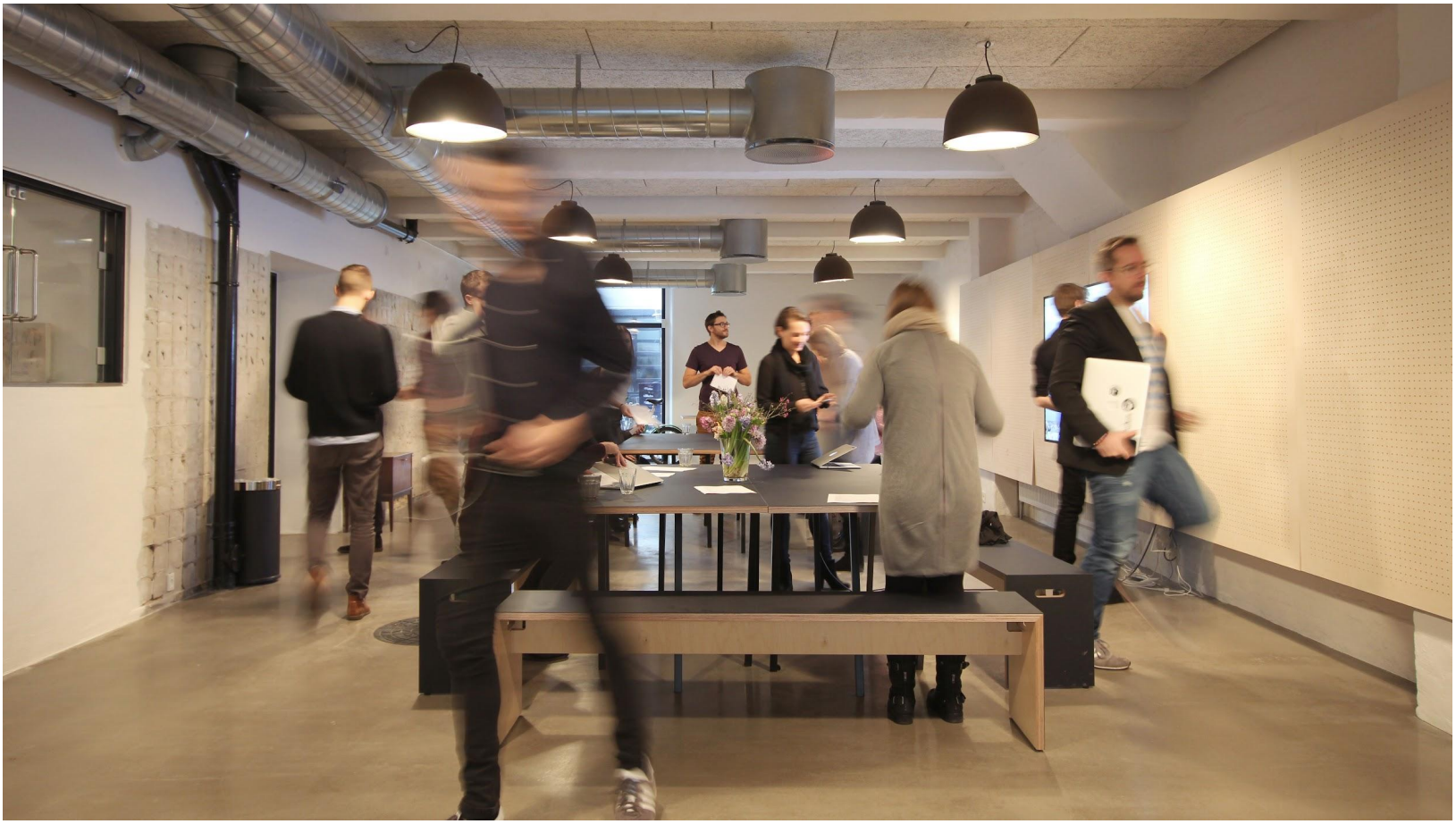

Table of Contents

Overview and Introduction

This document details the Security Policy and Practises at TwentyThree. It details how we work, but it is also made public for Information Security Officers and other interested parties working with current and prospective customers of TwentyThree. It is not intended as a legal document between TwentyThree and its customers; rather it documents the consideration going into the development, deployment and operations of the TwentyThree platform.

Any information found in this document should be considered as general purpose. Please refer to our Terms of Service and your particular agreement details for guarantees, liabilities and specific operations and security details.

The Security Policy and Practises are outlined in three distinct sections covering different levels of our security practises:

Infrastructure and System Operations: The TwentyThree platform is made up from a number of distinct services, hosted and operated by TwentyThree and our subprocessors. This section covers how this infrastructure is operated, updated and secured.

Development, Deployment and Monitoring: Our product software offering is continually updated, which involves a number of security considerations around best practises for building, testing, updating and monitoring software.

Security Awareness, Redundancy and Continuity: This final section covers the ongoing steps to enforce and test this security policy through specific policies, through employee training, and through redundancy and continuity planning.

Infrastructure and System Operations

Data Ownership and Processing of Personal Data

Data ownership is governed by the Terms of Service for TwentyThree, but as a general rule customers retain ownership and responsibility for all content hosted and published on the platform. Under the Terms, rights to the content is shared with TwentyThree to the extent needed in order to operate the service.

In addition, use of TwentyThree may include the processing of personal data governed by regulations such as the EU's General Data Protection Regulation. We operate the service in accordance with the security and compliance requirements in this regulation, and usually customers will explicitly direct our personal data processing by signing TwentyThree's standard Data Processing Agreement.

Security Architecture

The TwentyThree platform is designed around the principle of least privilege. All access control settings, file system access privileges, network port access et cetera are off by default, and enabled only for operational purposes with the minimum subset of resources necessary. Such privileges are idempotently managed by a central configuration management process.

By design, any component of the platform not designed from a security perspective to persist its state in accordance with the security guidelines set forth in this document is considered stateless. As such, any non-stateful component holds no customer data at rest.

The access of platform components to and from the public internet is delegated to several reverse proxying servers, such that no application instances or infrastructure components are directly reachable from the public Internet.

Unauthenticated contexts, such as the public web page, are isolated from the authenticated context at the network level. Additionally, infrastructure layer contexts are isolated at the network level to strictly isolate the potential reach of a given breach. As such, no infrastructure configuration is accessible from the application context and vice versa.

Physical and Environment Security

TwentyThree is built for secure, resilient and efficient data storage and hosting. The service is operated out of ISO/IEC 27001:2013 certified data centres located in the European Union.

Our primary hosting provider at the time of writing is Amazon Web Services in Dublin, Ireland, and changes are governed by the subprocessor notification policy details in our data processing agreement.

No currently running TwentyThree services require physical access to data or server centres from operation personnel. Should it be deemed necessary however, the granting or revocation of physical must be approved by management, logged including the justification for the access, and the access list will be reviewed at least quarterly.

Configuration Management

By design, all services underpinning the TwentyThree platform apply the described security architecture idempotently by being fully defined in, and controlled by, a configuration management system. The source of truth for the configuration management is providing a full history of changes in system configuration.

Configuration of network and storage equipment is manually managed, with all details of the configuration fully documented in a version controlled source repository, providing full history and audit trail of the configuration of the equipment.

Network Security

The TwentyThree platform employs a strict paradigm of strongly separated network layers to provide a base level of security. System management of physical infrastructure components are separated from the production networking layers by being a physically separate network accessible through an independent access point. In addition to our extensive internal security measures, TwentyThree employs a third-party service provider to perform scans across the TwentyThree platform centered around the OWASP 2013 and 2017 security guidelines.

Backup

TwentyThree should not be considered an asset backup service, and we advise all customers to maintain their own backup of valuable content. Having said that, data integrity is ensured at TwentyThree on by snapshot backups and all deleted objects are retained for a minimum of 30 days after deletion. Recovery is tested at least quarterly.

Non-volatile databases are continuously backed up to a cloud storage provider using a reasonably aggressive streaming of updates such as the continuous persistence of write-ahead logs at 10 minute intervals at most, as well as full database snapshots at scheduled intervals. This ensures full retention of all non-volatile databases for up to 30

days, allowing for point-in-time recovery to the granularity level supported by the underlying database. Under normal operating conditions, the worst-case recovery precision is 10 minutes. All data is transmitted to and persisted at the cloud storage provider using asymmetric encryption on the TwentyThree side. Recovery is tested at least quarterly.

Non-volatile databases are synchronously replicated onto a failover replica in a different availability zone. Furthermore, snapshots of full databases are taken every 24 hours. This ensures full retention of all non-volatile databases for up to 30 days, allowing for point-in-time recovery to the granularity level supported by the underlying database. Under normal operating conditions, failure of a database engine does not result in any data loss of data committed to the database. Recovery is tested at least quarterly.

System Logging

All requests to and in-band access of the TwentyThree platform is collected in a centralized logging system. Logs include, but are not limited to, HTTP/HTTPS requests, platform events, system events, security events from access or attempts to access individual servers. Collected logs are kept in a searchable index accessible to only personnel with the highest level of system access for a duration of time necessary to identify and investigate incidents. Logs are kept for at least 30 days.

In the case of a severe security event, a report will be forwarded to impacted customers at the discretion of TwentyThree and in accordance with our Security Breach Notification Policy.

Remote Access

Remote access to the application environment is reserved for the system operations personnel. Access is always encrypted, it is routed through dedicated jump hosts and firewalls, and all remote access requires public key authentication and/or two-factor authentication depending on target.

Remote access is controlled through our central configuration management regime meaning that access can be granted and revoked centrally.

Data encryption

Data stored on the TwentyThree platform is encrypted at rest whenever possible. Personal data such as real names, username and email addresses is securely encrypted by the

database systems, and the classification and categorization of personal data is detailed in our data processing agreements with customers. For performance reasons, we do not encrypt raw video and thumbnail image data at rest.

External data transit of sensitive data is, unless elected by the customer, always handled over HTTPS/TLS following industry recommendations for high-compatibility environments, or using other similar or stronger means of encryption depending on the protocol in question. Equally, all databases containing sensitive customer data are encrypted using 256-bit AES encryption at rest and require manual operation by a system administrator to be decrypted for use. This practise extends to all backups and other derivatives of the database.

Access management to TwentyThree systems

Access to the TwentyThree platform is restricted to an explicit need-to-know and need-to-access basis, and utilizes the principle of least privilege when granted. The system administrative team frequently monitors this access to non-application level components, which is idempotently enforced for all non-application level components using the configuration management regime described in this document.

We log when employees are granting or revoked access to personal data, including the justification for the access. Access lists are reviewed at least quarterly. Access to all TwentyThree systems and services that process data on behalf of customers must be protected with 2-factor authentication. In most cases this is implemented by using TwentyThree single sign-on gateway.

Updates and security patches

System administrative personnel actively monitor security bulletins for software used across the platform, including but not limited to relevant mailing lists and the Common Vulnerabilities and Exposures database. High risk vulnerabilities are sought to be mitigated as soon as the personnel becomes aware of them, while low risk vulnerabilities are mitigated as soon as it can be proven that such a patch does not impact the stability of the platform.

Non-security related software updates are applied in a continuous, rolling fashion to avoid any one update causing platform-wide interruptions.

Development, Deployment and Monitoring

Application Development and Testing

TwentyThree and internal development producers are built from the ground up for secure and manageable testing and deployment. First, all code and work on the platform is done on secured development instances by the developer team responsible for each service.

When code has been tested and verified the relevant commits are merged into the main code and pushed to a staging server, where further tests are run covering these same criteria, for example whether it introduces vulnerabilities or risks covered by the OWASP guidelines. Some of this testing is run automatically and as part of a Continuous Integration scheme, in which code is also subject to personal code review ahead of production release.

Deployment

Each service making up TwentyThree has a limited group of people with permissions to deploy to our production environments. All such deployment is managed by a deployment script that rolls out code slowly to avoid downtime – but each such deploy is triggered explicitly by a person-in-charge.

We monitor all services ahead of, during and after a deployment to verify that no bugs or vulnerabilities have been introduced. This covers logging of all code errors and authentication warnings along with general error rates, global response times and automated security scans. If a specific deployment is deemed to have compromised either of these metrics, there are procedures in place to roll back deploys again quickly.

Testing procedures span both automated flows and manual ones, and they cover both product deployment and system administration. These include, but are not limited to:

- Systematic port scanning;
- Systematic logging of systems usage and access;
- Testing for SQL injection;
- Error logging and error rate monitoring;
- Systematic scanning for XSS vulnerabilities;
- Personal code review;
- Quality assurance testing by a dedicated team.

Development and staging data

We do not ever use data from production nor personal data from our customers during development, testing or staging.

Security scanning

In accordance with the development guidelines described above, we perform automated, external security scans daily covering at least the risks, potential vulnerabilities and security recommendations detailed in the Open Web Application Security Project (OWASP) recommendations. This includes application vulnerabilities such as code and SQL injection; broken authentication; cross-site scripting; security misconfigurations and more.

Global Content Delivery Network

The TwentyThree global content delivery network is delivered in cooperation with Fastly and Amazon Cloudfront, and spans the globe with servers strategically placed on five continents. This platform provides a scalable front-end for the service delivery of video and photo assets alongside the actual page content and page resources (i.e. graphics, thumbnails, scripts, stylesheets) directly from the visitor's geographical location. This ensures optimised web delivery around the world as an integrated part of TwentyThree.

Data on TwentyThree is hosted and managed from within the EU.

The Fastly CDN currently covers these locations:

- *North America:* Ashburn, Atlanta, Boston, Chicago, Columbus, Dallas, Denver, Houston, Los Angeles, Miami, Minneapolis, Montreal, New York, San Jose, Seattle, Toronto, Vancouver
- *South America:* São Paulo, Santiago, Rio de Janeiro
- *Europe:* Amsterdam, Frankfurt, London, Madrid, Paris, Stockholm
- *Africa:* Cape Town, Johannesburg
- *Asia:* Chennai, Dubai, Hong Kong, Mumbai, Osaka, Singapore, Tokyo
- *Australia and New Zealand:* Auckland, Brisbane, Melbourne, Perth, Sydney, Wellington

The Amazon Cloudfront CDN currently covers these locations:

- *North America:* Ashburn, VA; Atlanta, GA; Boston, MA; Chicago, IL; Dallas/Fort Worth, TX; Denver, CO; Hayward, CA; Hillsboro, OR; Houston, TX; Jacksonville, FL; Los Angeles, CA; Miami, FL; Minneapolis, MN; Montreal, QC; New York, NY; Newark, NJ; Palo Alto, CA; Philadelphia, PA; Phoenix, AZ; Salt Lake City, Utah; San Jose, CA; Seattle, WA; Toronto, ON; Vancouver, BC ; Querétaro, MX
- *Europe:* Amsterdam, The Netherlands; Athens, Greece; Berlin, Germany; Brussels, Belgium; Bucharest, Romania; Budapest, Hungary; Copenhagen, Denmark; Dublin, Ireland; Dusseldorf, Germany; Frankfurt, Germany; Hamburg, Germany; Helsinki, Finland; Lisbon, Portugal; London, England; Madrid, Spain; Manchester, England; Marseille, France; Milan, Italy; Munich, Germany; Oslo, Norway; Palermo, Italy; Paris,

France; Prague, Czech Republic; Rome, Italy; Sofia, Bulgaria; Stockholm, Sweden; Vienna, Austria; Warsaw, Poland; Zagreb, Croatia; Zurich, Switzerland.
- *Asia:* Bangalore, India; Bangkok, Thailand; Chennai, India; Hong Kong, China; Hyderabad, India; Jakarta, Indonesia; Kolkata, India; Kuala Lumpur, Malaysia; Mumbai, India; Manila, Philippines; New Delhi, India; Osaka, Japan; Seoul, South Korea; Singapore; Taipei, Taiwan; Tokyo, Japan.
- Australia & New Zealand: Auckland, NZ; Melbourne, AU; Perth, AU; Sydney, AU.
- *South America:* Bogota, Colombia; Buenos Aires, Argentina; Rio de Janeiro, Brazil; Santiago, Chile; São Paulo, Brazil.
- *Middle East:* Dubai, United Arab Emirates; Fujairah, United Arab Emirates; Manama, Bahrain; Tel Aviv, Israel.
- *Africa:* Cape Town, South Africa; Johannesburg, South Africa; Nairobi, Kenya
- *China:* Beijing; Shenzhen; Shanghai; Zhongwei.

Monitoring

All services that make up TwentyThree are monitored internally, and we compute metrics both for availability and performance. In addition, access to external-facing services is monitored using Pingdom. For both of these monitoring regimes, all incidents are assigned to the on-duty systems operations team for resolution.

TwentyThree is a cloud-hosted platform with TwentyThree assuming full responsibility for the maintenance and systems administration of the platform. For this reason, we routinely:

- Make status reports and event information publicly available through the dedicated TwentyThree Status Page at https://status.twentythree.com
- Make uptime and availability monitoring available at http://uptime.twentythree.com

Third Party Services

TwentyThree relies on a number of third party services for the delivery of our service. A subset of these third party services handles and processes personal data on behalf of us and our customers -- whenever this happens, they are characterized as a Data Subprocessor and subject to our Data Processing Agreement. A list of all current subprocessors is available at https://www.twentythree.com/subprocessors where you can also subscribe to be notified of changes to the list.

Please refer to your signed Data Processing Agreement with TwentyThree for the specific details of legal obligations related to the use of third-party services for processing of personal data.

Security Awareness, Redundancy and Continuity

Security Awareness

TwentyThree maintains a strict set of Security Awareness Guidelines which is used for training all people joining the company. All new employees receive training within 45 days of joining the company, and the entire team receives mandatory, annual training on the guide. The guidelines themselves are reviewed and revised annually by management.

The security awareness guidelines and training covers (amongst other subjects):

- Authentication and Password Management, including our requirement to 2-factor authentication when accessing any system containing and/or processing customer data.
- The requirement for all computers and mobile devices issued by TwentyThree to employ full-disk encryption.
- That we guard against viruses by only allowing company devices to run software approved by Apple using their Security & Privacy feature.
- Best practises related to online encryption and use of wifi networks.
- The need for ongoing patching of software and operating systems.
- Policies related to reporting and actions if a device is lost or stolen.
- Office security best practises include rules governing the use of removable media and prohibiting sharing of access to the office.
- Risk classification schemes used within the company.
- The confidentiality rules covering all employees and related to all customer relationships.

Confidentiality

TwentyThree ensures that all employees are contractually bound by confidentially as related to customer relation and to personal data. Personnel receive appropriate training on their responsibilities and have executed written confidentiality agreements with obligations that survive the termination of the personnel engagement.

Service Level Agreements

A dedicated service-level agreement covering the use of TwentyThree is available on our Enterprise price plan and by agreement with the responsible account manager. The service-level agreement must be signed by TwentyThree.

Personal Data Breach Notification

Under the GDPR and by policy TwentyThree is required to inform data controllers and the relevant regulatory body within 72 hours of finding out about a breach of personal data. We consider the 72 hours is the final cut-off point, and aim to inform both affected customers and regulatory bodies as soon as possible.

Whenever possible, we will consult with our customers (acting as data controllers) to allow regulatory notification to happen jointly.

"Personal data breach" under the GDPR covers "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the company".

This breach policy and checklist serves as planning for the eventuality. As the Working Party state in that guidance, "controllers and processors are ... encouraged to plan in advance and put in place processes to be able to detect and properly contain a breach, to assess the risk to individuals, and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned when necessary. [...] To aid compliance with Articles 33 and 34, it would be advantageous to both controllers and processors to have a documented notification procedure in place, setting out the process to follow once a breach has been detected, including how to contain, manage and recover from the incident, as well as assessing risk, and notifying the breach".

In the event of a personal data breach, individuals for whom data is held must also be notified if the data leak is seen to pose a danger to their rights or freedoms, and unless it involves a disproportionate amount of effort to inform each individual. In this scenario a public announcement would suffice. TwentyThree acts as a data processor. Here, our role is to equip customers with the necessary information and context to contact individuals in the best possible way.

The specific process and policy for risk assessment, mitigation and communication in the event of a personal data breach are set forth in TwentyThree's Personal Data Breach Notification Policy.

Document change history

- 1.0, April 2018: First public version of this document.
- 2.0, January 2020: Second version reflecting changes on backup and policies.
- 3.0, October 2020: Updated document to reflect changes in cloud hosting platform.

- 3.1, November 2021: Clarification of security awareness and security practises.