Information Security

An overview of how 10to8 approaches Data Security

Version: 1.9_01 [External]

Introduction

Security is at the heart of 10to8. We are ISO 27001 certified by BSI, our servers are SOC 2 audited, and we provide a HIPAA and EU-GDPR ready service. We maintain best practice in information security and stay aware of the regulatory obligations we have; to our customers, users, and suppliers across the world. Our customers in banking, healthcare, and government count on it.

This paper outlines some of the measures that we have in place to maintain the security of our customers' data.

IS 705787

This document

Information Security 1.9_01

Your responsibilities

It is important to understand that 10to8's security doesn't guarantee your organization's security. Likewise 10to8's regulatory compliance does not stop your organisation from using 10to8 in a non-compliant manner. Security provisions, however extensive, cannot guarantee data security. Hence we act to minimize risks. A risk to your organisation arises from using any third party software.

It is always the ultimate responsibility of your business to manage your customers' and businesses data. We're here to help. That's why we built tools to help manage HIPAA and GDPR issues as well as making sure we're ISO27001 certified. DPAs and BAAs are available on request. We work with many customers on their particular requirements for data management.

Some key areas where it is your responsibility to minimise your risk are:

- To know what data you will be sharing with 10to8 and why:
    - Making sure that you do not use 10to8 to store special categories of data unless you have agreed it with us in advance;
    - That you only share the minimum necessary data with us to allow us to provide our service.
- Making sure your staff are appropriately trained. That they aware of what data can and can't be used in any system, and are familiar with good data security practices (such as strong passwords)
- Ensuring that if special categories of data or sensitive data are stored in 10to8 that the appropriate controls and features have been activated within 10to8 (talk to us, we're here to help).
- Managing consent for how 10to8 handles your users' data. Note we have tools that can help manage consents if you do not have an existing system for handling this. - Responding to users' rights requests under GDPR, HIPAA or other frameworks such as to know what data you hold on them. 10to8 has specific tools to help with such requests.

Information security policies

10to8 maintains a set of information security policies governed by ourInformation Security Management System (ISMS). This is as part of our, externally audited, ISO 27001 processes. The scope of ourISMS is: *"Data related to the development, provision, support and maintenance of cloud and API based Software as a Service for scheduling, booking and reminding appointments"*.

All policies are actively used, managed, accessible and audited. Each policy or group of controls has objective measures attached to their performance so that we can measure and ensure our continuous improvement. Regular audits of each policy of information security and the ISO 27001 are carried out as per ourISMS and supervised by our senior management team.

Organisation of information security

10to8's key objective for data security is to protect 10to8 Data: To ensure that it is kept confidential, intact (not modified or corrupted intentionally or by accident), available in appropriate circumstances (e.g. product provision) and is accessed to the minimum amount necessary for any required task.

To that end, we have:

- Information security roles and responsibilities clearly documented and communicated
- Separated duties and processes to evaluate performance to prevent conflict of interest
- Processes for ensuring knowledge of appropriate regulations and legal obligations

- Clear information security procedures in applicable workstreams (such as development)
- Policies are enforced that enable secure work on 10to8 systems
- A minimum necessary principle applied for access to all 10to8 Data and Systems

10to8 is committed to continually improving our systems security and improves the way we manage security to match the changes that we see in the business and how our customers use our systems.

People

In any organisation people, particularly human error,represent the greatest potential risk to data security. At 10to8 we recognise this and take steps across the entire employee lifecycle to minimise these risks.

Relevant, trusted, access

Access to any 10to8 system, tool, or data is granted only if: it is required; the individual has demonstrated the appropriate levels of skill; and after any appropriate training has been carried out by the individual. Access is logged and evaluated (minimised) on a continuous basis.

Training

10to8 runs regular Data handling, Data Protection and Regulatory Compliance training for employees. These are open to everyone in the company and run especially for the benefit of new joiners. At minimum we carry out one session for all staff each year.

Employee lifecycle

Employees are vetted on joining the business and training is given and logged on their joining. Following our onboarding process, where they are given the minimum necessary access to Data and systems to allow them to carry out their job. This is extended and changed as their responsibilities grow as part of our CPD processes. On leaving we have a rigorous process to ensure that access to all systems is revoked and any data that may have been retained is destroyed.

Asset & device management

We maintain an inventory of the information that 10to8 holds, including your business data and the data that you input on your customers. This includes all devices that may access 10to8 systems for which logs are stored and updated on a regular basis.

10to8 has strict policies that are monitored and enforced to ensure that devices that have access to business data are secure and that the data that could be accessed is limited (see network security). Devices are inspected regularly to ensure that they are free from Malware, lock after a short period, have a secure password and are encrypted according to our encrypted-at-rest requirements (AES-256).

We retain client data only insofar as it is necessary to fulfil our obligations to clients to provide the 10to8 service; and to the extent that it is necessary in order to comply with the laws and regulations of the client and users' country.

All client data, including that client's user data, is deleted/destroyed under our Data Destruction policy;

- after 1 year of client-account inactivity
- on deletion of the client account

Third parties must have equivalent or higher standards for Data Storage;
Third parties must have all appropriate agreements with 10to8 as per local legal requirements (e.g. Signed BAA, DPA).

Please note that it is not, generally, possible for 10to8 staff to access 10to8 customers' data. In the event that access is required for compliance with local laws or enquiries for example under HIPAA right to access requirements there are logged processes and notification procedures (as required) that are followed.

Access control

Secret Authentication Information is any thing that is used by a 10to8 employee to prove who

they are using an electronic system. For example, usernames, passwords, MFA codes, and private keys.

Each employee has an electronic identity for all internal and external systems. Employees do not share logins. Forthird party services, if they are sensitive then each 10to8 employee must create their own individual accounts.

New Employees & Identity Management

Issued with ID and training on password and identity management

Third Party Services

Guides to how to ensure security

Passwords

Passwords should match the sensitivity of the information they grant access to AND the risk of that information being accessed by an adversary, third party, or non-authorised user. In general all access should be through MFA (Multi Factor Authentication).

Cryptography

We use strong encryption for all data in transit, and at rest. In transit includes VPN for staff access and HTTPS for client access to our systems along with a rigorous key management system.

In transit cryptography

- OpenVPN Keys used by staff to access our VPN, encrypts data that is potentially highly sensitive, including customer data and software code Uses RSA 2048 bits
- HTTPS certificates used by 10to8.com to secure highly sensitive customer data and secret authentication information. RSA 2048 bits.

At rest cryptography

- RDS DB encryption keys used to encrypt data at rest in our production system, to guarantee confidentiality and integrity of customer data.
- Encryption standard is AES-256
- Keys are refreshed frequently

Physical security

10to8 ensures that the Physical working environment provides adequate and appropriate protection to 10to8 data and is safe and secure for our staff and visitors. Physical security measures include:

- A Secure, defined, security perimeter
- Entry controls with keyfob access
- Design of facilities that include allocated desks and a clear desk policy
- Redundancy and testing against external and environmental threats
- Device maintenance and inspection
- Strict Rules for unattended devices and screens locks
- Equipment lifecycle management including supervised disposal

Operational security

Procedures

One goal of 10to8 is to build self-organising teams. To do this we run an Agile process of development with a workflow and clear processes. These processes include:

- Change and capacity management policies to ensure product continuity and integrity - Management of critical programming interfaces (We treat internal programming interfaces as critical because it improves the stability of 10to8,reduces risk and allows us to deploy more often and more freely).
- A clear separation of development, testing and operational environments to minimise the risks associated with production data being used in a testing environment.

Logging and control

- All appropriate event logs are stored, maintained and reviewed.
- Logs are protected from tampering and alterations tracked
- Sysadmin logs are protected and reviewed
- Controls for software usage on operation systems are limited; access to this capability is limited and deployments are carried out via preconfigured scripts that can rollback any changes.

Vulnerability management

- Subscribed to info on relevant libraries and have scans regularly
- Process in place to react to new vulnerabilities as they are discovered
- Conduct Regular(at least annual) penetration testing by a third party

Information Security 1.9_01

Communications security

10to8 restricts the transfer of sensitive data to the minimum necessary and only when encrypted in transit and arrest. We know that communications security extends beyond data storage and transfer to how the organisation communicates and coordinates its activities and so we have a set of guides and training to protect against these risks.

For example to ensure the security of electronic messaging, meaningful communication is limited to two-way multi factor authenticated channels. This means that, for example, email is not used to convey company information unless corroborated over a second communications channel.

Network controls

10to8 manages no network equipment on site. We rent servers, network connectivity etc from secure third parties such as AWS and manage them to ensure they comply with our requirements for data security. Only members of the engineering team who have received relevant training are allowed to manage network systems.

VPC & VPN - All network traffic in and out of our networks are encrypted according to our Cryptographic Keys Policy in order to safeguard the confidentiality and integrity of this data. Access is logged.

System development

New developments are assessed against security objectives before they are worked on.

To ensure secure best practice we use standard, simple and boring mechanisms and practices to write and maintain safe software. We do not attempt to build our own security software ortake novel approaches. Our standard tools, including Python and Django, come with many security features that we use. Additional measures are taken to protect against unlawful disclosure or interception and alteration.

We are careful when adopting third party suppliers and libraries, considering the risks they introduce and whether they are compatible with our legal,regulatory and contractual obligations.

Our development procedures include:

- Change control processes,

- Reviews of applications after changes
- Restrictions on changes that can be made to the system by person and process
- Secure system engineering principles that are shared and regularly reviewed -
A secure development environment (see 10to8 network diagram)
- Regular system security testing including third party penetration testing at least annually - Use of fictional test data (no production data used in a testing environment)

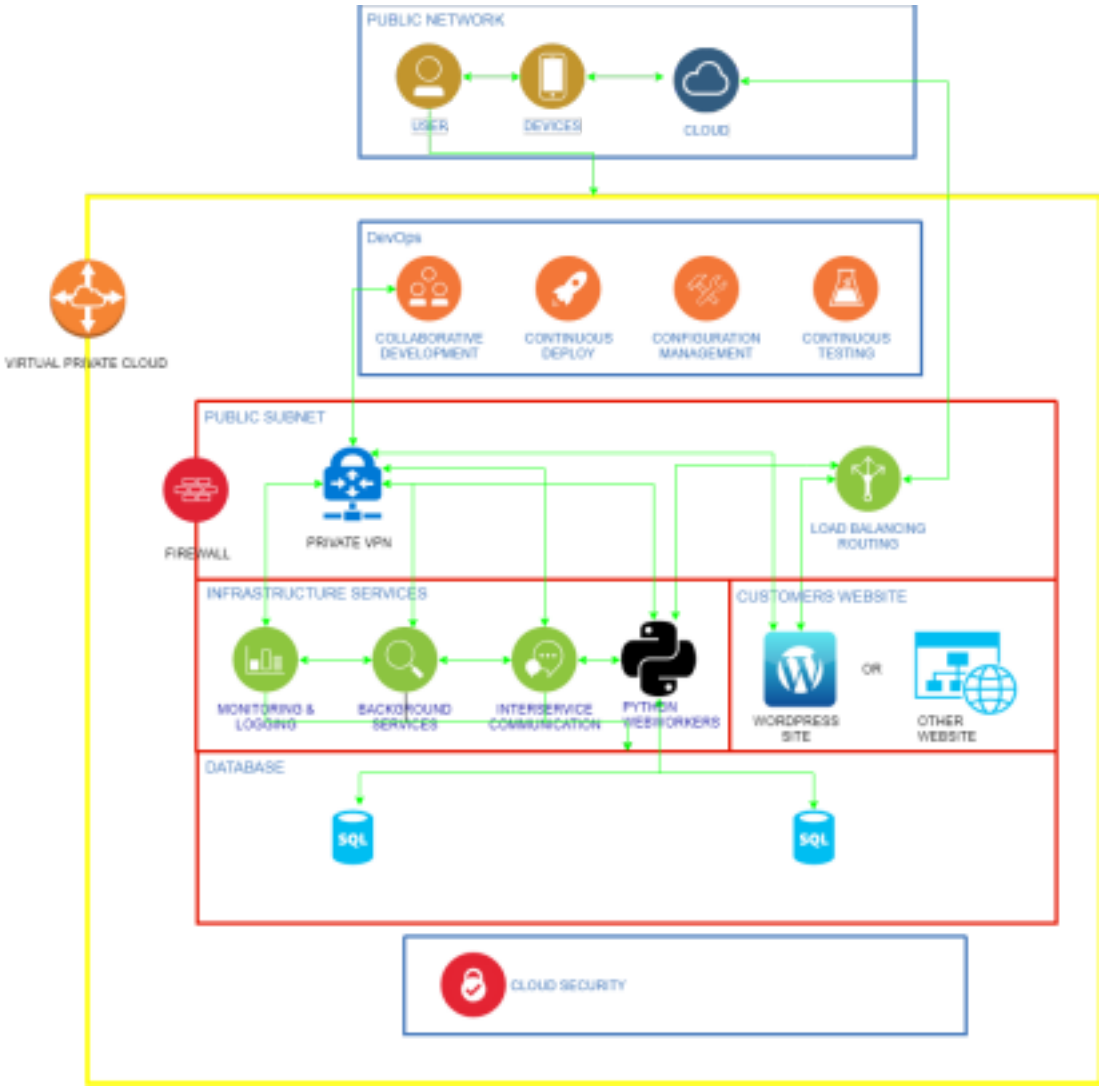

Figure 1 - 10to8 network diagram

Information Security 1.9_01

Supplier relationships

We hold our suppliers to the same high standard of data security that we hold ourselves to. There are actively managed processes in place to ensure that information shared with suppliers matches our security commitments to our customers. All supplier relationships follow our simple Document, Check, Secure, Limit process.

Access of third party systems to customer data is kept to a minimum (following our minimum necessary principle) and documented along with and contractual agreements and security controls deemed necessary. This is reviewed at least annually.

An example of this in action is for HIPAA enabled accounts: if you have an account with HIPAA tools enabled certain third party services will be automatically limited. Usually this is because those suppliers are unable to provide a signed BAA protecting PHI.

For key suppliers such as AWS whom we use for data infrastructure and servers we have in place: SSAE 16, SOC 2 reports, ISO 27001 and PCI DSS.

Incident management

10to8 has designed processes to act fast in the event of a data incident. We have a simple and thorough incident process that is regularly tested: Initiate, escalate, investigate,report, evaluate & prevent.

Any entity that is affected by a data incident is notified according to this process. This includes businesses, users, and statutory authorities such as data regulators. This means that in the event of a data incident you will be told quickly and given the information you need to act according to your own policies and processes.

All staff are trained in its operation and all incidents are logged and treated as a serious data breach until shown not to be. The process itself has been iterated over the course of many drills.

Continuity management

We maintain continuous backups and regularly test our ability to provide a continuous service in the event of any anticipated disaster.

Backups:

- Daily backups of the system (snapshots) - can be restored in 5 minutes to a point in time the day prior to failure
- Point in time backup recovery - can be restored within an hour to a point in time including all data up to five minutes prior to the failure

We test the recovery of these backups as part of our disaster recovery process.

Continuity & disaster recovery

This section lists ways that 10to8's product can fail, and how we recover from them. We test each of these modes of failure to check we are able to recover from them fast. These are tested at least annually and where applicable the results are benchmarked against our contractual requirements.

- Contractual Requirements
- Disaster recovery
- Database failure
- Server failure

- Data centre failure

Compliance

10to8 complies with applicable legal and regulatory requirements, maintains ISO 27001 accreditation, and follows industry best practices for data protection and data security. 10to8 is EU GDPR and HIPAA ready.

Our data infrastructure allows us to ensure that user data and organization data stays in the regulatory area required; for example on an account with a set provision location sensitive personal data would not leave that country or regulated region (in the case of the EU).

We actively seek out upcoming changes to regulations and aim to implement product and internal changes before our customers are affected by them: 10to8 maintains an up to date & regularly reviewed set of regulatory requirements that are applicable to our customers' data. This list includes the recent applicable legislation,regulatory bodies and reporting requirements.