Information Security Plan v3.1.3

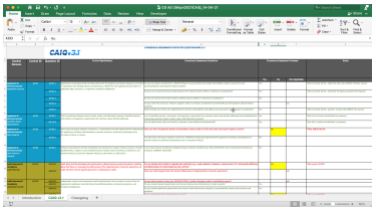
Introduction

Correctly handling our clients' data is essential. Clients trust us to hold valuable data on their behalf. We need to comply with relevant laws as a minimum, but, in addition, we take all precautions to ensure that we securely handle data with the greatest of care.

This document describes the technical and organisational measures that are in place to ensure CustomerGauge fulfils its role as a secure and trusted partner (as well as GDPR compliant Data Processor).

How to use

The document structure follows that of Consensus Assessments Initiative Questionnaire (CAIQ) version 3.1 https://cloudsecurityalliance.org/



- To understand what data CustomerGauge captures (from our websites and product) and how we use it, please see our **Privacy Policy** here: https://customergauge.com/privacy-policy/
- To read or **Service Level Agreement** which includes our **Business Continuity Plan** see here: https://support.customergauge.com/support/solutions/articles/5000789667-customergauge-service-level-agreement
- For our **Terms of Service or Data Processing Agreement** contact Customer Support

Document Info

This document follows the structure of the Cloud Security Alliance's (CSA) **Consensus Assessment Initiative Questionnaire v3.1 (CAIQ) https://cloudsecurityalliance.org/research/cloud-controls-matrix/**

The CAIQ consists of a comprehensive list of 300+ questions relating to cloud security. It was chosen as our preferred structure as it provides a mapping to 38 other competing standards.

Co-Editors

CEO Adam Dorrell, COO/HR Camilla Scholten, CFO/Legal Erik Biekhart & Hila Altman, VP Tech Antony Laycock

Version History

- v1.0 September 12 2014: Created
- v1.1 April 7 2015. Added privacy policy and Business Continuity plan
- v1.2 Jan 7 2016. Added Disaster Recovery Plan
- v1.3 Feb 9 2017: Reviewed by AL/AD, Added additional details on changes to APIs, upgraded security items on AWS, updated links
- v1.31 Feb 13 2017: Updated links - made most public
- v1.4 Refresh Based on RFP FAQ
- v1.41 Format refresh following move to Confluence
- v1.42 Added some information based on RFP experience. Attached AWS DPA / SendGrid Model Clause.
- v1.43 13 April 2018 Minor Edits
- v2.00 Updated to reflect GDPR compliance. De-duplicated information between Privacy Policy, SLA, Terms of Service and DPA
- v2.10 29/04/19 Yearly Review Updates
- v2.11 09/05/19 Update following May Infosec Team Meeting
- v2.12 02/03/20 General Refresh - Hardening and Cognito now mentioned.
- v2.13 29/07/20 A few extra clarifications based on common questions and recent improvements
- v3.0 10/03/21 Restructure Based on CSA – CAIQ
- v3.1 30/11/21 Six month refresh
- v3.1.1 22/06/22 Half Year refresh
- v3.1.2 08/08/22 Page header update
- v3.1.2 24/01/23 Added Docker under Static Analysis tools and supplemented IAM-11.1

01: AIS - Application & Interface Security

AIS-01 Application Security

Software Development Lifecycle

CustomerGauge follows an Agile development process. Each new User Story is analysed, designed and tested taking into account a JIRA maintained list of ongoing Non-Functional Requirements, including Data Security requirements.

Coding

As best coding practices we follow the OWASP Secure Coding Practices. We also offer employees with technical security responsibilities with membership of OWASP in order to share knowledge.

There is a focus on integrating security requirements into the SLDC rather than adding them pre or post release. However, there is dedicated time (currently one sprint per quarter) in our delivery roadmap dedicated to addressing security issues.

80% of our back-end code is based on PHP, 20% based on Python and NodeJS/Typescript. We don't use any third party suppliers for source code development, though we may occasionally supplement our Development Team with contract programmers. Contract programmers will be treated as part of the development team and will be subject to the same processes and checks.

Static Analysis

The following static analysis tools are used regularly:

- Docker: Trivy, Clair AWS ECR image scanning, AWS Inspector
- PHP: PHPStan, Roave Security Advisories, PHPCS
- Node: NPM audit, ESLint
- Python: MyPy, Bandit

All new code is subject to peer review. (On GitHub Pull Request) Security Requirement review is within scope.

AIS-02 Customer (i.e. Client) Access Requirements

Prior to granting Client access to the CustomerGauge system a mutually binding Data Processing Agreement (DPA) must be in place. Our Terms of Service act as a default version of this, and we can supply a model version. Many clients have their own DPA, which CustomerGauge then co-signs.

AIS-03 Data Integrity

All data import and entry features have Data Validation checks in scope.

AIS-04 Data Security / Integrity

The five principles and seven security pillars of the AWS ‘Well-Architected Framework’ is used for architectural guidance.

02: AAC - Audit Assurance & Compliance

CustomerGauge is working towards SOC 2 Type II. We are happy to share audit reports with our clients, on request.

AAC-01 to 02 Independent Audits

We have yearly Independent Technical Audits in place:

- with a globally recognised 3rd Party Penetration Test organization (currently Secura)
- with a local AWS DevOps specialist who checks for AWS Architecture security best practices

Recurring contracts are in place with both. Reports are shared with Clients on request.

AAC-03 Information System Regulatory Mapping

Ad hoc processes are in place whereby each department keeps up with regulatory changes. For example, the recent **Schrems-II** judgment where the EU Court invalidated **Privacy Shield** resulted in the Technical Department by adding ‘Migration to EU data centres’ to the roadmap and the Legal department updating DPAs (now completed)

03: BCR - Business Continuity Management & Operational Resilience

BCR-01 Business Continuity Planning

CustomerGauge operations have been designed to be highly resilient and for Business Continuity from the ground up.

Office Infrastructure

The office infrastructure is entirely cloud based, using best of breed services such as Salesforce, Google, Atlassian etc. Therefore, no corporate network is required and, with the use of MFA, employees can work securely wherever they have a private internet connection.

The office WIFI offers internal and guest networks, both being secured by password.

Although the organization can function in 'WFH' mode effectively, we do also have a 'warm office' alternative for our Amsterdam HQ, which is approximately 3km away and is fully equipped with alternate internet, power, light, heat, and space for at least 8 key workers. This is ready to go 24x7.

In case of temporary power outage all workers have laptops and can continue for several hours on batteries.

As proved during COVID in 2020/2021, CustomerGauge is able to function in an entirely remote way.

BCR-02 Business Continuity Testing

Database restores and enforced remote working are tested many times per year. Covid restrictions was the most recent extreme example of the latter - the entire CustomerGauge workforce went from office based work to homeworking with two days notice with zero operational impact.

The CustomerGauge platform makes use of AWS managed 'Aurora' RDS. We use parallel reader and writer servers for improved performance and high availability. AWS regularly upgrades the server which includes swapping the reader and writer, thus testing the failover mechanism

Note that we are a Multi-Tenant system so there is some sharing of cloud resources, though each tenant does have a separate database within the shared RDS. So, although failovers would be triggered for all tenants in the same region it is possible to restore specific tenant databases back to a known state.

We make use of a 3rd Party uptime monitoring tool which provides a public webpage. This can be found here: Realtime CustomerGauge Uptime Status (Pingdom)

Documentation

Key information regarding operating the CustomerGauge platform safely and securely is documented on the intranet (hosted using Confluence from Atlassian). Page restrictions are used to limit the availability of sensitive information.

In addition, all Cloud Resources are created via automation. So 'Cloud Formation' template give very precise documentation of the existence and setup of each resource.

BCR-03 to 08 Data Centre Resilience

Environmental, Power & Telecoms Supply, Location & Maintenance

The product cloud infrastructure is 100% AWS based and makes use of Multiple Availability zones. (An AWS 'AZ' is one or more data centres, within a region, that are geographically separated from other data centres within the same region. The separation needs to be far enough to such that a natural disaster could only affect a single AZ. Hence the majority of failures will not impact availability.

AWS Managed Backups are made across these availability zones such that in the case of a natural disaster taking out the datacentres in one availability zone, then workload would automatically be shifted to a different zone.

See here for their resiliency measures: https://aws.amazon.com/compliance/data-center/controls/

BCR-09 Impact Analysis

Service Level Agreements are in place for the CustomerGauge platform (Medium Impact) and the public Surveys modules (High Impact).

BCR-10 Policy

The CustomerGauge Service Level Agreement document is available to prospects and clients

BCR-11 Retention Policy

Tenant Data Retention

Tenant Data is hard deleted within maximum of 30 days of their contract ending. The CG platform also provides facilities such that our tenants can delete specific records within their data set, for example to comply with GDPR requests.

We provide a Certificate of Destruction on request. Request Procedure and Certificate of Data Deletion for details.

Backups

All Relational Database Systems have AWS Managed Backup schedule enabled. This creates daily and incremental Backups that can be restored to a specific point in time, accurate to within a minute. We sometimes receive requests from tenants to restore certain data that may have become polluted by human error. We hence test our backup restore mechanism several times a year as a part of ongoing operations.

'Multi Availability Zones' are enabled which means that the Backup location is independent of the location of the system being backed up.

These backups will be deleted automatically one month after creation.

Diagnostic logs will be automatically purged within two months of client platform activity ceasing.

Retaining Machine Images

The CustomerGauge architecture is based on 'Serverless' technology and so the CustomerGauge product does not make use of virtual machines, hence there is no need for AMI retention policy.

04: CCC - Change Control & Configuration Management

CCC-01 New Development / Acquisition

New Cloud Resources, including Data Stores, are created strictly using 'Infrastructure as code'. This means it is subject to the same peer review process built into our coding workflow.

CCC-02 Outsourced Development

CustomerGauge does NOT make use of outsourced development on the CustomerGauge product.

CCC-03 Quality Testing

Quality Assurance (QA) is an integral part of the Development Process, not a pre-release bolt on. Product Owners and QA specialists will help specify test scenarios which will be coded into Unit Tests wherever possible. Developers are expected to test their own work before passing on to others. The final acceptance test will be performed by the feature / fix sponsor, so typically QA specialists, Product Owner or a Customer Support representative.

All this is controlled by a Defect tracking workflow managed in the ‘Atlassian Jira’ ticketing system.

There is a bi-weekly cross functional team review and prioritisation process for all open defects. Lower priority ‘Known bugs’ are recorded in an Archive project which can be exported on request.

The build process excludes non-production code, such as unit tests, from the final image.

Diagnostic logging has four levels, INFO, DEBUG, WARNING, ERROR. All four are enabled for ‘DTA’ systems but lower levels are excluded from production.

CCC-04 Unauthorized Software Installations

Employees receive training in how to recognise and avoid unsafe software installers.

CCC-05 Production Changes

Features and Fixes are bundled into bi-weekly releases use Jira ‘Fix Version’. Source code changes relating to these are peer reviewed as part of our GitHub workflow. The Components affect are added to the Jira ticket so that a manifest of production modules to be changed can be produced. This manifest is used to assess the extent of regression testing needed.

All production changes are actually implemented by automated build and deployment pipelines, triggered by merging the tested ‘DTA’ branch with the ‘Master branch. Only tickets that are marked as 'Acceptance Tested’ may be merged.

Our build process includes dependency scanning tools (currently Dependabot) that inform of new versions being available, or current versions being newly tagged as vulnerable. We use the DTA environment to test version upgrades before allowing them onto the Master branch.

Database schema upgrades are automated (currently using PHP ‘migrations’) across all tenant databases in order to keep them in sync and maintain a standardized product.

On a strictly exceptional basis, database edits can be made in order to repair corrupt data. This requires three internal levels of approval (Business, Product & Technical) plus Client signature if relevant.

05: DSI - Data Security & Information Lifecycle Management

DSI-01 Classification

Each Tenant’s Data is stored in a separate database, but on a shared Relational Database Server per region. Regions are isolated from each other. There is no data security classification required at server level.

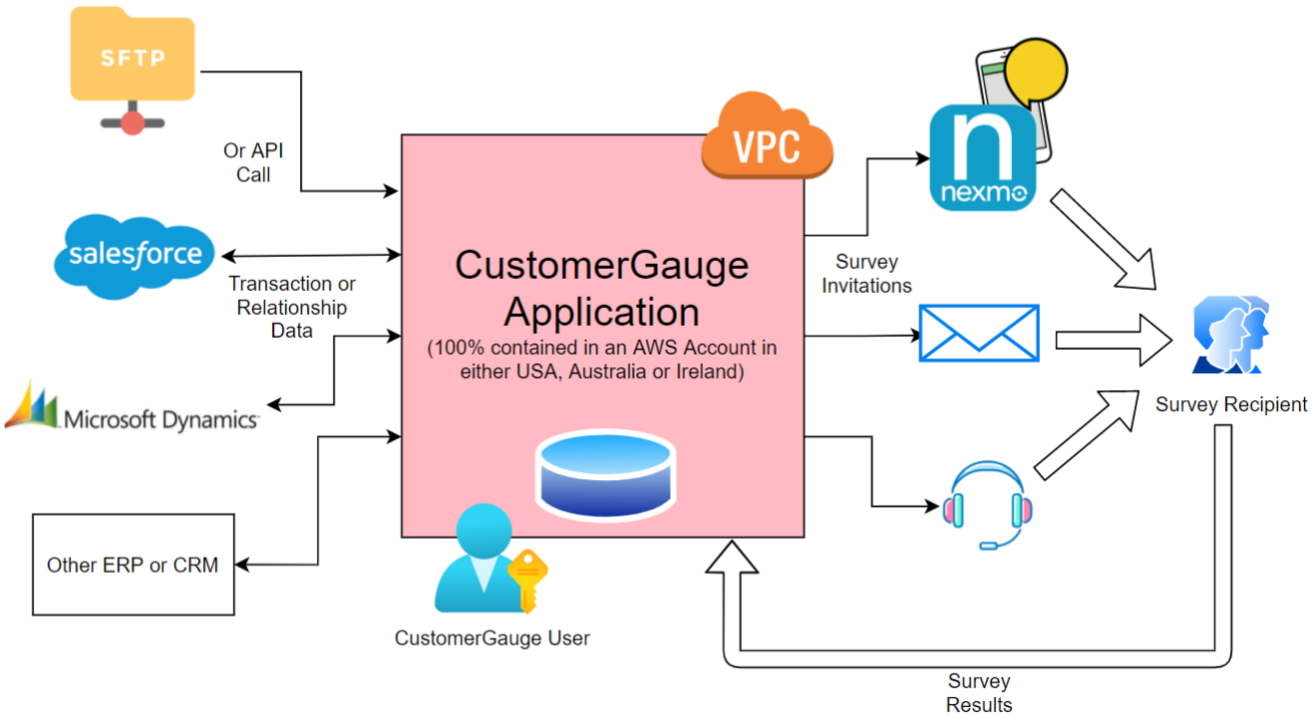
However, tenants do have the flexibility to define what data is relevant to their business process and therefore uploaded to CustomerGauge. A meta-data feature is available that allows the tenant to define whether a data item is ‘personal' (e.g. Name & Address) or 'shared value personal’ (e.g. Gender). This allows the CustomerGauge platform to provide appropriate anonymisation behaviour.

Cloud Resources are created by CloudFormation scripts which can also be used to set tags on each resource.

DSI-02 Data Inventory / Flows

CustomerGauge platform operates in three, completely separate and unconnected regions. (See Data Centre Security section below). Clients can choose which region they would like their data to be hosted in at onboarding time.

Data is stored in AWS managed RDS in AWS VPC. Data from which surveys should be generated can be imported from various ERP / CRM systems either via a dedicated integration, Webhooks, API call, SFTP file drop or manual import. Survey invitations are sent via SMS (Nexmo), Email (AWS SES) or Voice Call (Icon). Invitations contain minimal personal information, just enough to deliver the invitation. Survey responses are captured within the CustomerGauge application and can only be accessed by authorised CustomerGauge users. Though it can also be optionally pushed back to the originating ERP / CRM system via a dedicated integration or via a webhook.



Data Collection

The CustomerGauge platform can function with a bare minimum of data being exchanged (e.g. just an email address or SMS number). But to get the full power of our reporting and analytics suite our clients usually choose to provide or request much more. This data falls into two categories:

- Data provided by our client. That relates to survey recipients (e.g. Company, revenue, person title, geo segment, Product Purchased segment etc) in order to allow our clients to search for patterns in response data. The data uploaded will typically vary by the touchpoint being surveyed or reported on.

- Data provided by survey recipients. Provided as part of answering a survey. Survey/survey questions are defined by the client. (e.g. Net Promoter Score, Drivers, Free text comments)
- Surveys do not track any personal information, beyond what is asked explicitly in the survey itself, using cookies or other techniques. The only cookie used is a ‘session’ cookie that:
    - Keeps track of which page the survey recipient is viewing
    - Enforces that a specific survey instance can only be completed via invite url

DSI-03 E-commerce Transactions

The CustomerGauge platform does not deal with e-commerce transactions. But data in transit and at rest is protected by open encryption technologies. (AES256 & TLS 1.2+)

DSI-04 Handling / Labelling / Security Policy

The CustomerGauge system offers a meta-data export of the standard data model. This can be used to understand the import data structure. However it does not utilise a data-labelling standard as clients are free to flex the usage of fields within type limitations.

DSI-05 Nonproduction Data

There is a policy in place that forbids employees to copy any production data, that may contain personal information, to test environments. Furthermore, the platform does not provide tools to facilitate this.

In the rare event that it was essential in order to reproduce a high priority, elusive bug then the procedure is to first make a copy in production, then run an anonymisation process, and only then copy to DTA.

DSI-06 Ownership / Stewardship

The CustomerGauge platform acts as a GDPR ‘Data Processor’. This means that we don’t have any ownership or stewardship of our clients' data. There is a signed ‘Statement of Work’ process available if a customer requires us to edit their data, but the scope must be specified precisely.

GDPR right to revoke permission

CG platform does not store highly sensitive data such as credit card or national id numbers by default. However, it is possible for clients to choose to load sensitive date in our 'User defined fields'.

To comply with GDPR’s right to revoke permission, the platform offers an 'anonymise' API available that will replace personal data with '****'. This anonymise process will include User Defined Fields where the user has indicated their type to be 'Personal Data'. Alternatively, users can simply choose to delete records associated with certain contacts.

DSI-07 Secure Disposal

Customer data held in CustomerGauge product

In case of service termination CustomerGauge will permanently delete the full client database within one month of contract ending (or sooner if explicitly requested).

AWS Managed RDS will ensure that the data is unrecoverable once backups are deleted (one month after database is deleted).

06: DCS - Datacentre Security

The CustomerGauge product is hosted in AWS Data Centres (Ireland-EU, North Virginia-USA, Sydney-Australia). Details of AWS Data Centre Security measures can be found here:

https://aws.amazon.com/compliance/data-center/controls/

DCS-01 Asset Management

Cloud Resources are managed by automation, not manually. All resources are created and configured by 'CloudFormation' scripts. These scripts effectively act as an asset register and are configuration controlled in a source control system.

Resources that are deemed to be Business Critical are configured with 'Auto-Healing' or Multi-Availability Zone attributes.

DCS-02 Controlled Access Points

AWS provides physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) to safeguard sensitive data and information systems.

DCS-03 Equipment Identification

The CustomerGauge platform offers three levels of IP Allow list protection which can be used to provide external access protection based on geographical location.

Regarding equipment identification, the CustomerGauge architecture makes use of 'Serverless' resources. This means that the connections made to our AWS accounts arrive at an Application Load Balancer and, from there, AWS takes care of mapping those requests to the appropriate virtual & physical servers, (which are not managed by CustomerGauge).

DCS-04 Offsite Authorization

The CustomerGauge policy is that data & resources hosted in an AWS region must be kept in that region. There is no procedure in existence for transferring them offsite.

DCS-05 Offsite Equipment

The CustomerGauge platform does not use any on-premise resources.

Employee Devices

An asset register of employee devices is maintained. At end of life the assets are physically destroyed or a witnessed factory reset and data wipe performed.

DCS-06 Policy (for safe & secure working environment)

Employee attendance at regular Security training sessions, which include safe and secure environment best practises, is registered. We hold these every 6 months, and include a quiz element to reinforce learning. New employees have this as part of their induction procedure.

DCS-07 to 09 Secure Area & Assets Access & Authorization

Access to data centre secure areas is completely managed by AWS data centres. The CustomerGauge platform does not use any on-premise resources.

CustomerGauge employee office has a private entrance that is secured by a metal shutter. The inner door is access controlled by key card. Entry and exit times of each key card are recorded and stored for 90 days.

07: EKM - Encryption & Key Management

EKM-01 to 02 Entitlement & Key Generation

CustomerGauge only makes use of AWS managed encryption keys. There is a separate encryption key for each cloud service that we use. These keys are stored in AWS KMS (Key Management Service).

As we are a multi-tenant platform, we do not make use of tenant specific encryption keys. Encryption is applied at the Relational Database Server level.

EKM-03 Encryption

All data at rest is encrypted using AES256.

We do not make use of virtual machines so there is no concept of encrypted data migration between them. (Though in general, data entering and leaving our VPC is encrypted).

EKM-04 Storage and Access

Using AWS KMS does mean that the keys are stored with the same cloud provider as the resources. However, AWS managed keys have an extra layer of hardware protection that means they are not available, even to AWS employees. https://aws.amazon.com/kms/features/

08: GRM - Governance and Risk Management

GRM-01 Baseline Requirements

CustomerGauge's 'serverless' architecture means there is no physical or virtual infrastructure within our control, so version control of OS, hypervisors etc is the responsibility of AWS. However, we can monitor the versions in use from the AWS console.

GRM-02 Risk Assessments

A ‘Risk Council’ gathers every quarter to review the existing security risk list to check which risks were addressed since last meeting and for any status or priority changes.

This meeting also discusses new risks that may have come to light:

- Technical
- Procedural
- Legal & Statutory

GRM-03 Management Oversight

Managers are included in the regular Employee Security Training courses. They are responsible for their team members' ongoing compliance.

GRM-04 Management Program

This document and its references form the basis of the CustomerGauge Information Security Management Program.

It is made available to Clients and Prospects on request.

Updates are made as frequently as necessary, to register significant changes, with six monthly updates as minimum.

GRM-05 Management Support / Involvement

The ‘Risk Council’ includes C-Suite level executives and its decisions are documented in an issue tracking system.

GRM-06 Policy

This document and its references / attachments forms the basis of the CustomerGauge Information Security Policy. It is modelled on the CSA CAIQ standard but the medium term goal is to attain SOC2 certification.

There is currently no dedicated member of staff with the title of Security Officer, so this document is co-written by members of the executive team, who each have their specialist area relating to security. (e.g. Technical, Product functionality, Legal, HR).

The document is approved at CEO/COO level.

This document may be shared with Prospects, Clients & Partners. Partners must agree to comply with this document or their own equivalent.

GRM-07 Policy Enforcement

Employees receive regular security training and are made aware of the sanctions that may be imposed in the case of deliberate or regular infractions.

GRM-08 Business / Policy Change Impacts

The findings of Risk Assessments (GRM-02) often result in re-prioritisation of technical roadmap work. However, the findings could also result in procedural changes.

GRM-09 Policy Reviews

Irrespective of risk assessment findings, this ISP will be reviewed and updated at least annually. Customers will receive notification of major updates.

GRM-10 Assessments

The bi-monthly risk council review inspects the current data security risk list. Items are (re)assessed and re-prioritised based on:

risk factor = likelihood of occurrence x potential damage

GRM-11 Program

Formal documentation of above is in progress.

09: HRS - Human Resources

HRS-01 Asset Returns

Handover of company-owned assets is part of the ‘Leavers Checklist’ described in HRS-04. This must be completed before end of business on the last day of service.

HRS-02 Background Screening

Minimum of two professional or academic references are sought for new hires. Where the legislation allows it we do proactive employee screening.

HRS-03 Employment Agreements

Employment contracts contain clauses relating to adherence to Data Security Policies. These must be signed before employees are given access to data resources.

HRS-04 Employment Termination

A 'Leavers Checklist' is maintained that lists the superset of systems and resources to which employees have access. Each item on this list must be marked as 'Removed' or 'Not Applicable' by Office Administration / Leavers' Managers by end of last employment day.

The checklist template itself is reviewed at least annually in case new systems / resources have been added to its scope.

HRS-05 Portable / Mobile Devices

The portable device policy is that sensitive or personal data should never be stored on mobile devices.

'Acceptable Use' policies are defined to reduce the risk of viruses that might be used to intercept keystrokes on website access for example.

HRS-06 Non-Disclosure Agreements

Employees sign Non-Disclosure agreements as part of their employment contract.

HRS-07 Roles / Responsibilities

Our standard Data Processing Agreement clearly defines that CustomerGauge clients act as GDPR Data Controllers and that CustomerGauge itself acts as a GDPR Data Processor.

HRS-08 Acceptable Use

All employees are provided with the computing assets they require to perform their role. There is no 'Bring Your Own Device' policy. Team managers have authority to approve 'safe use' of personal devices in exceptional situations (e.g. whilst waiting for corporate hardware to be repaired)

HRS-09 Training / Awareness

All employees are required to attend a CustomerGauge Security Training course. This course is refreshed and repeated at six month intervals. Attendance is tracked.

The course covers NDA obligations, Basics of GDPR from Data Processor perspective, Accessing Client Data and importance of 'Clean Machine', Password Management, Secure data sharing, Physical security, Social engineering, Safe Website use, Anti-Virus use, Remote Working.

HRS-10 User Responsibility (i.e. CustomerGauge Employee)

Employees are made aware of their data security obligations in their employment contracts and in regular security training.

HRS-11 Workspace

A ‘clean desk’ policy is in place regarding sensitive documents.

Devices must have session timeout and lock screen enabled, minimum 30 minutes.

10: IAM - Identity & Access Management

IAM-01 Audit Tools Access

The main audit tools in use are AWS CloudWatch / CloudTrail, for cloud resource logging, and an ELK stack (Elasticsearch/Logstash/Kibana) for application logging.

User access is based on least privilege principle and approved by the VP of Development (or deputy). Kibana access is based on GSuite SSO.

Access logs are available for AWS accounts and anomalies are detected by AWS ‘Guard Duty’ service.

IAM-02 User Access Policy

Access Removal

A formal ‘leaver process’ is in place. It includes a checklist of system access points. Access is removed on completion of the employee's final day with the company. Every system must either be explicitly marked as ‘n/a' or have access removal confirmed. At this point we also verify that the checklist itself is current and a new version prepared as necessary.

Employee Access to Customer Data

CustomerGauge employees must adhere to a policy of not accessing client data unless by direct delegation for specific maintenance requests from clients. This process is managed and audited via our ticketing systems.

When permission to access data is given, via a ticket being raised to investigate a problem, the Employee will access the CustomerGauge platform in the same way as a regular admin user, but with a dedicated CG-Support or CG-Tech username.

CustomerGauge operates a 'clean machine' policy i.e. Client Data should not be transferred to employee laptops or printed out, in fact it should never leave the cloud. However, if, in the course of handling a maintenance request, it was essential to transfer client data to laptop, say to diagnose a problem in an export function, then this data must be removed by end of business, same day, at the latest. Data should never be transferred onto removable media.

If a copy of some data needs to be logged on the internal or external ticketing system (e.g. as a screenshot) then personal data must be obfuscated.

A Least Privilege mechanism is in place that allows Department Managers to define only certain groups of staff are allowed to access certain pools of Tenants.

Database Access

Occasionally problem investigations require access to the personal data stored in the product's relational Database directly. Again, this must be covered by a request in the ticket system. Database logins are personal and granted with limited permissions based on role. The Relational Database Server is hosted in a Virtual Private Cloud so access is only possible by SSH into a Bastion Host. Each Tenant has a separate database that needs to be connected to individually.

Cloud Account Access

Multi-Factor Authentication is a mandatory setting for all technical staff.

Removal of Access

Typically completed on last day of contract. Can be accelerated if the termination was not amicable.

IAM-03 Diagnostic / Configuration Ports Access

Managed via AWS account access as authorised by VP Development.

IAM-04 Policies and Procedures (IT infrastructure)

Managed via AWS account access as authorised by VP Development. Four levels of access are allocated according to the needs of the employee's role. 1) No Access. 2) Read Only Access 3) DevOps Access 4) Admin Access. These levels can be applied on a per AWS Account basis.

Note that there is no corporate network. All corporate applications and data are managed by 3rd party SaaS providers that can be accessed over the internet. MFA use is compulsory if offered.

IAM-05 Segregation of Duties

The CustomerGauge platform offers several layers of access control for its users, all of which can be controlled by User Admins. Full details are available on the support site, but in summary.

- Role (e.g. Admin, User, Workflow User) controls access to features within the platform.
- Division (e.g. By Tenant Business Unit) controls access to data within a User Organization's hierarchy.
- Group (e.g. Department) similar to Division but can be based on a client's choice of grouping dimension.

IAM-06 Source Code Access Restriction

Source Code is stored and managed in a private Enterprise GitHub account. Developer access is authorised by the VP of Development. There are over 100 code repositories and so access can be denied or granted at a fine level of granularity.

IAM-07 (Unauthorised) Third Party Access

Quarterly Risk Council meetings are held to review all security risks including unauthorised third party access. Mitigations can be scheduled based on the combination of 'Likelihood x Impact'.

Unauthorised Access checks are also in scope of the annual Penetration test.

Custom Domain Sending

CustomerGauge can send email invitations from a default customergauge.com sending address OR from a tenant defined (sub)domain, e.g. surveys.example.com.

If the latter option is chosen then the owners of the domain need to edit their DNS records to show that CustomerGauge, via AWS SES are authorised to send from that domain. The DNS values they use will be generated, and be specific to, the CustomerGauge AWS Account / Region. This ensures that other Third Parties, that may also hold an AWS SES account, are not also authorised to from the customer's domain.

IAM-08 User Access Restriction / Authorization (Employees)

Cloud Resources

For safekeeping, our root account is held by our Certified AWS Support Partner.

VP of Engineering and a few authorised deputies have Admin access.

In general, Developers and Tech Support have write access.

Some selected employees have read-only access.

New logins can only be created with Approval of VP Engineering or an appointed Deputy.

AWS IAM is used extensively to ensure 'System Logins' only have access to the resources they require.

Database Access

Only approved on a least privilege principle, by Department Managers.

Access can be separated on a Database / Region / Read Only basis.

Each authorized user has a unique username and password.

IAM-09 User Access Authorization (Partners, Clients etc)

Tenant Access

Director of Customer Success Department can authorize groups of support staff to access groups of tenants e.g. by region or data sensitivity. This mapping is managed via 1Password vaults. Even authorized users still require tenant permission to access their data on a support case by support case basis.

An audit log of CustomerGauge Admin activity is captured. It can be shared with Tenants on request.

Partner Access

No Technology Partners have access to Tenant Data.

Where a CustomerGauge platform has been sold by a reseller partner then that Partner shall provide Support services as described in this document.

IAM-10 User Access Reviews

AWS account user access permission reviews are performed at least quarterly.

IAM-11 User Access Revocation

As described in HRS-04, user access is de-provisioned on last day of employment or on change of internal role.

Platform deletion/offboarding of churned customers is executed within one month of contract end and ensured by a double check procedure each month.

IAM-12 User ID Credentials

Internal Corporate

Cloud Account Access (AWS)

Employee Access is authorised by VP of Development. Least Privilege Principle is followed. MFA is mandatory. Policy Enforcement, covering people and resources, is in place using AWS IAM.

Tenant User Account

- Users are created by User Admins.
- Users' username & email are the only mandatory fields.

Tenant Admins can allocate Tenant Users a Role, a Division and a Group. These attributes will control scope of data access.

CustomerGauge Platform Managed Authentication

On invitation, users are sent an email containing a ‘create account’ link. Hence there is no ‘default password' or ‘force change on first login’ option.

- The authentication process is based on a traditional username/password combination.
- Passwords are hashed and salted using SHA-256
- User Password Policy **REQUIREMENTS**
    - Special Character (except: @, #)
    - Small Case Character
    - Upper Case Character
    - Number

  - More than 8 characters
  - No sequential numbers
  - No username, last name or company
- The system is locked after five failed access attempts. User Admin intervention is required to unlock the system.
- User Credentials are stored encrypted in 'AWS Cognito' User Management service which provides secure password reset option without requiring Support. **CustomerGauge Employees should never be aware of Users' Passwords**
- Note: the above Authentication rules are standard across the CustomerGauge platform. They cannot be modified on a per tenant basis.

Multi-Factor Authentication

MFA is available via our SSO options. MFA directly on CG platform is on our development roadmap.

External Authentication (i.e. SSO)

Various SSO options are supported, typically those that are SAML based, supported by AWS Cognito, see Support site for the current list.

IP Restrictions

The CG platform offers the possibility to restrict access to a trusted list of IP addresses. Admin users will find a module "Security" in the admin menu and they are able to enable/disable the feature providing a list of IP addresses.

Enabling the feature the system will perform an additional check during the authentication process and deny the access in case the client user's IP does not match with the whitelist. Whitelists can control:

- User Access to the CG platform
- Programmatic Access to the APIs
- Visibility of the 'Digisign' Slideshow Report

IAM-13 Utility Programs Access

The CustomerGauge platform is running 100% in an AWS managed VPC, using serverless technology resources, so attack vectors based on utility programs accessing virtualised partitions do not present a significant risk.

11: IVS - Infrastructure & Virtualization Security

IVS-01 Audit Logging / Intrusion Detection

Cloud Account Access (AWS)

Employee access to the AWS accounts is logged using AWS IAM, CloudTrail and CloudWatch.

CustomerGauge Platform Access

- 'UAC' (User Access Control) logs are maintained for login attempts, password change events etc.
- User Action logs are maintained to provide an audit trail of configuration changes made by regular users.
- User Admin Action logs are maintained to provide an audit trail of configuration changes made by User Admins.
- CustomerGauge Admin logs are maintained to provide an audit trail of configuration changes made by CustomerGauge internal tooling. These internal tools are accessed by employees by using GSuite SSO.

Note that the contents of these logs are not directly accessible via the CustomerGauge platform. However they can be provided in csv format on request.

Automated Access Review

An Intrusion Detection System (AWS Guard Duty) is enabled.

IVS-02 Change Detection (Virtual Machine Images)

The CustomerGauge platform is running 100% in an AWS managed VPC, using serverless technology resources, so attack vectors based on tampering with virtual machine images do not present a significant risk.

IVS-03 Clock Synchronization

All servers are synchronised by AWS using their Time Sync Service.

IVS-04 Capacity / Resource Planning

Processing Capacity

The CustomerGauge platform is hosted on serverless resources, either AWS Fargate (container management) or AWS Lambda (Function as a Service). Both are configured to auto-scale rather than rely on pre-planned over-capacity.

Database Capacity

Our Relational Database Servers (RDS) are not yet capable of auto-scaling, though they can be manually, vertically rescaled at short notice due to their High Availability configuration.

In general, we aim to run RDS at 50% overcapacity vs peak time.

IVS-05 Management - Vulnerability Management (Virtual Machines)

Serverless technology depends on AWS micro-virtual machines (Firecracker). These are completely managed by AWS and are created and terminated many times a day, thus avoiding the risk of virtual machines being compromised.

IVS-06 Network Security

See diagram in IVS-09 for current network architecture.

WAF

A Web Application Firewall (WAF) is in place. Over time it will have extra rulesets enabled to provide ever increasing levels of security. Each proposed increment will be created, prioritised and tracked in the Tech Department ticketing system.

IP Allow List

Internal technical staff that require VPC access can have their home IP added to an IP allow list, subject to Department Manager level approval. The allow list is managed via an AWS Security Group. Each entry is documented and the list is regularly reviewed.

IVS-07 OS Hardening and Base Controls

'Hardening' is the process of securing a system by reducing its surface of vulnerability.

Since CustomerGauge architecture is based on serverless technology, our 'hardening' is focussed on our AWS Fargate containers.

We make use of a standard, ultra-lightweight 'Alpine' base container image.

We use 'Dependabot' dependency scanning tools to minimise the libraries we depend on. Where possible libraries will be statically rather than dynamically linked in order to provide explicit control of upgrade timings.

IVS-08 Production / Non-Production Environments

Our Production environment is in a completely separate AWS account than the DTA (Dev, Test, Acceptance) and Research environments.

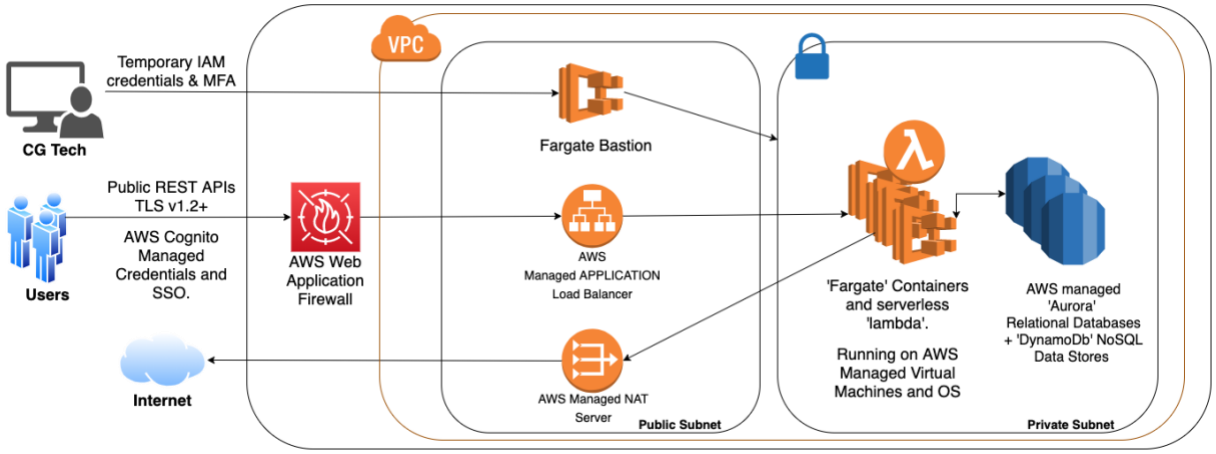
Where Tenants would like to make use of a test environment, we will create an extra platform in the Production account so that there is no chance of personal data being stored on DTA.

There is a policy of no production test data ever being copied across to DTA environment. As the name suggests, DTA is a test environment and its security / stability can not be guaranteed at all times.

IVS-09 Segmentation

AWS Account

AWS hosted data and resources are deployed within an AWS Virtual Private Cloud that performs a similar function to a firewall.



The VPC can only be accessed from the internet via an IP locked Bastion server.

Production databases can only be accessed from within the VPC, or via the Bastion from CustomerGauge offices or from approved employee home IP addresses. (SSH Connection).

We use several AWS accounts in order to provide 'least privilege' role-based access rules. (Production, DTA, Shared Services, Billing, User Access Management, Research.)

Database Structure

There is a separate database per client (‘tenant’) in each RDS system. No RDS tables containing private data are shared with other tenants’ databases. Database passwords are generated by AWS and auto-rotated.

Only a single Tenant Database can be connected to within a session. Sessions are managed automatically from our PHP framework and stored into a Redis database. The Redis database is only accessible from within AWS or via Bastion host and whitelisted IPs.

CG has an automatic session expiration having an Idle Timeout set at 8 hours and an Absolute Timeout set at 1 day.

IVS-10 VM Security - Data Protection

CustomerGauge has no physical or even virtual servers so there is no server migration process in place.

If there is a need to migrate RDS data between AWS servers and/or accounts then AWS DMS (Database Migration Service) will be used to provide a secure transfer channel.

IVS-11 VMM Security - Hypervisor Hardening

Although there are no Virtual Servers or Hypervisors to manage, DevOps staff access to the Container Clusters is managed via least privilege principle using AWS IAM and MFA.

IVS-12 Wireless Security

The CustomerGauge offices do have password protected Access Points. Note that this is just to gain an internet connection; there are no corporate network resources.

IVS-13 Network Architecture

CustomerGauge fully relies on AWS network infrastructure. As company leader on cloud computing, it offers the most advanced certifications and it complies with most important standards on network security and IT management as ISO27001, ISO9001, SOC1-2-3.
Our account's servers are configured to only open ports specifically required for the application to function.

https://aws.amazon.com/compliance/data-center/controls/

AWS Shield is enabled to combat DDoS attacks.

The core components of the CustomerGauge architecture are running in a dedicated VPC (see diagram above)

We have an AWS Managed Web Application Firewall (WAF) in place.

Internally, the architecture is based on a microservices model such that the individual components can be auto-scaled & auto-healed independently using AWS CloudWatch availability alerts.

Core services are running in Docker Containers on ECS using Fargate clusters.

Inter-service communication is provided via queues (SQS) or pub/sub notifications (SNS) or Event Bus (EventBridge) for extra resilience.

12: IPY - Interoperability & Portability

IPY-01 APIs

The CustomerGauge platform provides an extensive range of standard, public (but requiring authentication) REST APIs.

https://support.customergauge.com/support/solutions/5000170913

An option to use Webhooks is also provided.

IPY-02 Data Request

In addition to the ‘GET’ verb being supported on the APIs described above, the CustomerGauge platform includes a Data Export feature supporting .xls & .csv file formats.

IPY-03 Policy & Legal

APIs and imports / exports generally are subject to the same SLA as the rest of the platform:

https://support.customergauge.com/support/solutions/articles/5000789667-customergauge-service-level-agreement

IPY-03 Standardized Network Protocols

The CustomerGauge platform supports TLSv1.2+

IPY-04 Virtualization

The CustomerGauge architecture is based on ‘Serverless’ technology. Any virtual or physical hardware is managed behind the scenes by AWS.

13: MOS - Mobile Security

Anti-Malware

Anti-virus protection is provided for all Windows and Apple mobile devices. By default a weekly scan is enabled. Admins can track that scans have been performed.

Employees are trained on how to recognise and avoid malware attack vectors.

(BYO) Device Control

CustomerGauge does not support a ‘Bring Your Own Device’ scheme. All employees will be provided with appropriate, company owned mobile devices.

Device Management can be handled by the employees (with access to an IT support channel) directly since there is a policy of forbidding sensitive data being stored on the device.

MOS-16 Passwords

Passwords must only be stored in the corporate account of a Cloud Based password management tool (currently 1Password).

Browser password management must be disabled or protected by a master password.

It is mandatory to use strong password rules. (See IAM-12)

- Laptops
- CSM & Tech logins to CG platform
- Logins to business critical applications

If an application offers MFA it must be used.

If strength rules can be edited on a user basis then they must be strengthened not softened.

14: SEF - Security Incident Management, E-Discovery, & Cloud Forensics

SEF-01 Contact / Authority Maintenance

Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies). These are handled through CEO and COO on ad-hoc basis

Physical Addresses

EUROPE: Van Diemenstraat 182B, 1013CP Amsterdam, NL
USA: 3 Burlington Woods Burlington 01803, MA

Request from authorised lawful entity for Data on individual.

COO will validate credentials of the requester before approving.

SEF-02 Incident Management

This document explains the measures we take to ensure your data is protected from illegitimate use. In the unlikely event that these measure prove insufficient we will follow an incident Response plan based on the standards in the "Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology" https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf , described below.

CustomerGauge detected data security incident.

We understand that our Clients, as Data Controllers, have a GDPR obligation to report data breaches to authorities and affected data subjects within 72 hours. As Data Processors, CustomerGauge will support this obligation.

With respect to monitoring, we use a DevOps partner (see Suppliers Section) to help manage our AWS account. They have a comprehensive set of alarms, including those that trigger on high levels of suspicious access activity. In addition, the CustomerGauge technical team makes daily use of 'Kibana' application logs.

In case of a suspected breach, the process will be :

- Member of CustomerGauge staff that suspects potential data problems will raise an internal ticket for the Tech Team to investigate.
- If confirmed the Head of Tech Department (or a deputy) will prepare an 'Incident Report' for the CustomerGauge Management Team.
    - Example of the internal **CustomerGauge Security Incident Response Form**.
- The Management Team will review the report and if the incident is confirmed will analyse the extent and impact. Client communication will be prepared and it will include the information required by GDPR breach reporting rules:
    - describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
    - communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
    - describe the likely consequences of the personal data breach;

- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Customers will be informed within a maximum of 24 hours of this information becoming available.

Data Incidents that do not involve a breach.

e.g. A system or hardware defect causes data pollution or deletion. This will normally be dealt with internally as our comprehensive backup system will facilitate a restore operation. However, if this was not sufficient to completely resolve the problem then the incident reporting process will be:

- Member of CustomerGauge staff that suspects potential data problems will raise an internal ticket for the Tech Team to investigate.
- If confirmed the Head of Tech Department (or a deputy) will prepare an 'Incident Report'.
- Affected Clients will be informed via Customer Success Department, or in severe cases, by CEO.

A review of any Low priority incidents is a recurring agenda item in the weekly ‘OpCom’ Management Meeting.

SEF-03 Incident Reporting

Your Customer Success Team representative is your first point of contact for any data security concerns. From there, the standard escalation path (dependent on severity) is:

- Customer Success Team
- Technical Team
- VP Engineering
- CustomerGauge management team
- CEO (available in 4 hours 24x7) for Severity 1

In the medium term we hope to appoint a DPO (Data Processing Officer) that will have security as their main remit. In the meantime the role is shared between members of the CustomerGauge Security Council (COO, CFO, VP Engineering, VP Product).

The escalation to Technical Department is via Jira ticketing system. Evidence of the Incident and history of steps taken to date must be attached. For urgent issues, VP Engineering, or a deputy, must also be informed by a direct messaging side channel.

SEF-04 Incident Response Legal Preparation

CustomerGauge supports single tenant litigation holds and data for subpoenas.

i.e. restoring a single tenant backup to a frozen point in time.

SEF-05 Incident Response Metrics

Summary statistical information regarding security incidents can be shared on request.

15: STA - Supply Chain Management, Transparency, and Accountability

CustomerGauge does not use 3rd party organizations to develop the platform's source code. If contractors are used then they will be treated as an integral part of the CG Development team and will be subject to the same rules as described in this document.

CustomerGauge takes responsibility that our Partners comply with the standards described here. We retain the right to change suppliers if necessary, though new Suppliers would be bound by at least the same security requirements.

STA-01 Data Quality and Integrity

We use the services of a 3rd party Hosting Support provider to act as an extension of the DevOps team outside of office hours.

Our jointly agreed policy is that the 3rd party provider may have access to the server systems but not the data they contain. Copies of the partner's Security Policies are available on request.

This partner also has individually named employee access to the CustomerGauge codebase in order to help diagnose any out of hours problems.

STA-02 Incident Reporting

Incident details will be specifically communicated to the tenants and partners that are identified as affected. via normal electronic channels. There are no plans to broadcast via portals, though we do provide a public uptime monitor.

STA-03 Network / Infrastructure Services

Capacity monitoring is handled by AWS Cloudwatch metrics. Capacity overload alarms are configured and are routed to the DevOps team via Slack.

STA-04 Provider Internal Assessments

CustomerGauge is currently working towards SOC2 certification. This will drive the policy and structure of the next wave of internal assessments.

Several Engineers have passed AWS Cloud certification exams. CustomerGauge provides time for studying and exam time.

STA-05 Third Party Agreements

CustomerGauge uses the following third party organizations in the delivery of its platform.

AWS

AWS is used for all application hosting. We use the following AWS Regions:

- EU - Ireland
- AsiaPac - Australia
- US - North Virginia

The Region may be selected by the client during the onboarding process.

Once selected, no data is transferred outside of this region.

CustomerGauge has a DPA in place with AWS Ireland. AWS_Data_Processing_Addendum__DPA___Self-Service___2016-12-12_ CG8March2017.pdf

Nexmo

Nexmo is a market leading SMS SaaS provider. They are based in the US and of course they distribute SMS globally. Their terms and conditions are GDPR compliant as they offer a zero data storage option. DPA is in place.

CloudElements

CloudElements is a SaaS provider that simplifies integrations with CRM & ERP systems such as Salesforce & NetSuite. It is US based but its use is optional from a tenant perspective.

Oblivion b.v. (Now part of Xebia Group)

Is an Operations partner and AWS Consultancy that help CustomerGauge provide 24/7 cloud incident coverage. A DPA is in place.

SendGrid

SendGrid is a US based email provider that has been integrated with CustomerGauge for several years.

However, due to the recent Schrems II case, we now have project in place to move to a different mail provider (AWS SES) which offers EU only hosting. We expect that our integration with SendGrid will be completely removed by mid-2022.

All existing suppliers, and any future suppliers are/will be selected based on their ability to comply with the geographical region choice of the tenant and comply with applicable legislation for that region. Where necessary, CustomerGauge legal counsel will review the relevant DPA.

Copies of these sub-processor agreements are available on request.

Declaration

CustomerGauge does not share tenant data with any third party organizations (other than those listed above to the extent required for operational reasons.

Neither does CustomerGauge make use of tenant data other than to collect anonymised, aggregated benchmark information.

STA-06 to 08 Supply Chain Governance Reviews

CustomerGauge is currently working towards SOC2 certification. This will drive the policy and structure of the next wave of third party governance reviews.

STA-09 Third Party Audits

CustomerGauge has a recurring, annual contract in place with a specialist Cyber-Security Organization to perform yearly Penetration tests. The most recent test was Nov 2021. The Executive Summary of this test is available on request.

16: TVM - Threat and Vulnerability Management

TVM-01 Antivirus / Malicious Software

All Employee Windows & Apple laptops are provided with a market leading Anti-Malware solution (currently Trend Worry-Free). The scan and update frequency of each machine is monitored.

Note that anti-virus software is not applicable for our cloud infrastructure. The ‘serverless’ architecture means that AWS are responsible for the virtualization and provisioning of resources. Typically, the ‘micro-VMs’ will be created and terminated many times per day. Each creation will use an up to date, freshly patched image.

TVM-02 Vulnerability / Patch Management

See STA-09 & TVM-01.

TVM-03 Mobile Code

The CustomerGauge platform is pure SaaS and only requires a JavaScript enabled Browser to be present on Users' machines.

There will be no other attempt to transfer software to install and run on a user’s machine.

Browser pages are protected by the following protocols / headers:

- HTTP Strict Transport Security (HSTS) to enforce https connections
- Content-Security-Policy (CSP) to restrict from which locations resources can be loaded
- X-Frame-Options & frame-ancestors to restrict the CG Application from being hosted in a frame and hence being vulnerable to click-jacking
- X-XSS-Protect Headers to protect older browsers from XSS attacks
- X-Content-Type-Options to protect against content ‘sniffing’