Beamery

Beamery Security Control

Version 1.1

Contents

Compliance & Trust

Security Standard

Certification	Status	Certificate
ISO 27001 Certified	Current	Certified: December 2019 Certificate Number: IS 715495 Auditor: BSI See our certificate here: https://docsend.com/view/ck7umec
Privacy Shield Compliant	Current	See our compliance here: https://www.privacyshield.gov/
SOC 2 (Type 1)	Pending (Q1 2020)	-

GDPR

Certification	Statement
GDPR Compliance Statement	https://docsend.com/view/945vqg9
Data Retention Strategy	https://docsend.com/view/fr4yibe

Data Center Locations

Cloud Provider	Purpose	Certifications	Location
Google Cloud Platform	Primary Hosting	ISO 27001 / SOC 2 / CSA https://cloud.google.com/certification	US East Region
Google Cloud Platform	Primary Hosting	ISO 27001 / SOC 2 / CSA https://cloud.google.com/certification	Europe (coming in Q3 2020)
Yandex	Localized Hosting	ISO 27001 https://cloud.yandex.com/security	Russia (coming in Q3 2020)
Amazon Web Services	Backup Site	ISO 27001 / SOC 2 / CSA https://aws.amazon.com/compliance/	US East Region

Beamery Office Locations

Country	Location
United Kingdom	London
USA	Austin, Texas / San Francisco, California

Introduction

Beamery's Information Security Management System (ISMS) has been established to secure business operations and ensure Beamery products protect its customers' information; maintaining their competitive edge to proactively attract, engage and retain the right talent. This is in accordance with the ISMS Statement of Applicability and includes all Beamery operational functions, cloud services offerings and physical locations.

Our security program reinforces Beamery's commitment to deliver world-class solutions via a secure, globally scalable platform. The external attestation of our security policy and controls is crucial for our customers and aligns us to industry best practice and standard.

Web-Application Security Controls

- Access to the beamery.com application is only via HTTPS (TLS 1.2 or greater) establishing the encryption of the session between Beamery end-users and the application.
- Customers can add & remove Beamery users from within the user control platform
- Single Sign-On (SSO) support via industry standard SAML 2.0 Identity Providers (IdP).
- Two-factor authentication (multi-factor authentication) for accessing Beamery is available with customer SSO.

Encryption

- Beamery uses AES 256-bit encryption for encryption at rest.
- Traffic between Beamery and any partner APIs is encrypted over HTTPS utilizing TLS 1.2 or greater and OAuth 2.0 where applicable.
- Backup files are encrypted at rest and in transit between primary and secondary storage locations.

Network

- Beamery utilizes GCP's network controls to restrict egress and ingress network access.
- We utilize multi-tier architecture including multiple and logically separated VPC (Virtual Private Cloud), DMZ, public, and untrusted zones within GCP.
- A centrally configured and controlled Web Access Firewall (WAF) is in place for all traffic between Beamery users and the application.
- We monitor network activity, this allows for detection of malicious attacks, intrusion etc. In addition, we also have monitoring solutions in place for engineers to visualise what is happening at any given moment.
- For Network hardening we utilise our cloud provider's VPC with private IP ranges and subnets and firewall rules. We also have IP tables as internal firewalls which can be automatically populated with network intrusion prevention rules. For infrastructure hardening DISA approves our cloud provider and performs regular audits.
- We remove default accounts and disable unnecessary ports and configuration

Monitoring and Auditing

- Beamery's systems and network are continuously monitored for security incidents, system health, network abnormalities, and availability.
- We conduct ongoing capacity and availability monitoring to ensure SLA compliance.
- Logging is automatically analyzed and reviewed to detect suspicious activity and prevent threats. Any anomalies are escalated as necessary.
- Beamery's Incident Response team monitors information.security@beamery.com and works according to our Incident Response Plan (IRP) when necessary.

Assess Control

- Access to the Beamery Production Network is restricted on an explicit need-to-know basis, utilizes least privilege, is frequently audited and monitored, and is controlled by our Dev Operations Team. Employees accessing the Beamery Production Network are required to use two factor authentication.
- Beamery's account security is monitored and maintained through the following measures:

    - IAMs access through GCP
    - Secure user credentials to development in Github
    - Restricted User access to Kubernetes Control
    - Restricted User access to MongoDB
    - Tripwire and Fail2ban on the cluster to catch any intrusions
    - Use private subnets in our VPC to restrict access to datastores to minimal instances
    - Minimising number of ports open to the internet

Vulnerability Management

- Beamery has deployed a technical vulnerability management policy to safeguard networked resources, internal devices and customer environments. Major application data flow ingress and egress points are monitored and we conduct routine automated port scanning and internal passive scanning. Results from these tests are reviewed by our platform engineering team.
- Beamery retains Cobalt.io and Bishop Fox to undertake third party penetration testing twice annually. The scope of these external audits includes compliance against Open Web Application Security Project (OWASP) Top 10 Web Vulnerabilities (www.owasp.org), external perimeter and our cloud security configuration.
- We perform weekly vulnerability scans against our staging environments covering OWASP Top 10 Web Vulnerabilities.

Incident Response

Any incidents on detection are moved for tracking purposes into the Beamery incident management system where a full timeline of events is logged in real-time. This includes the staff members involved, the type of incident, the resolution, and ultimately the reports generated based on what was detected.

Sub Processors

Beamery uses a small number of approved sub processors (including cloud hosting providers and data enrichment partners) in the provision of service to our Customers. Please see our current list here https://docsend.com/view/x9ajage. Beamery will notify customers 30 days in advance of adding any new sub-processor.

Security Working Group

Beamery SWG is a cross organisational operational security Group chaired by the SIRO and meets every 3 months to provide the necessary focus to manage the ISMS, to set and monitor objectives, review KPIs and control efficiency measurement. Any security incidents will be reviewed by the SWG to take appropriate actions to prevent where possible occurrences. All policies are reviewed by the SWG to ensure they remain consistent with business and ISO27001 standards. The SWG enforce a regular internal audit programme and review all reports and findings for non conformance and improvement opportunities.

Physical Security

- Beamery support teams operate from ISO27001 certified locations. Door access controls, 24/7 security patrols, CCTV and visitor procedures are in operation.
- Clear desk and clear screen policy applies whilst working within a secure Beamery support location. Where required privacy screens are used to prevent unauthorised access to sensitive data.
- Access logs are reviewed monthly to determine inappropriate access
- Local office networks are segregated by secure configured company wireless access points. Separate guest networks are provided where necessary
- Remote working policy is enforced for global remote support teams.

Asset Management

All Beamery support assets are centrally controlled and maintained to ISO27001 technical control standards of encryption, device harding, anti - malware and use of removable media outbound is blocked.

HR Security

- All support personal undertake required background screening up to and including fraud checks where required.
- All personnel permitted to access production level data are required to undertake CRB and international fraud checks.
- All personnel receive mandatory security training, DPA and regular phishing campaigns are launched to confirm end user awareness.
- Engineering teams undertake OWASP security engineering principles at least annually.
- All personnel sign the IT acceptable use policy and confirm the code of conduct and employee handbook by signing terms and conditions of employment. Non compliance to policy is enforced via disciplinary procedures.

Risk Management

Annual risk assessments are conducted against Beamery information assets to review control selection and risk reduction measures. Where applicable risk treatment plans are tracked and managed until identified risks are within SIRO approved tolerances.

Key Contacts

Data Protection Officer	privacy@beamery.com
Chief Information Security Officer	informartion.security@beamery.com
Beamery Legal	legal@beamery.com

About Beamery

Beamery's Talent Operating System allows enterprises to attract, engage, and retain top talent, and manage the entire talent journey through one unified platform. Beamery's mission is to help the world's best companies acquire their greatest assets: their people. Founded in 2014, Beamery is trusted by the world's most innovative global organizations to treat their candidates like customers. Beamery has offices in London, Austin, and San Francisco. For more information, visit the *Beamery website*, follow *@BeameryHQ* on Twitter, or email us at *info@beamery.com*.

"The best candidate experiences are powered by Beamery."

THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND IS PROVIDED "AS IS". BEAMERY DISCLAIMS ALL AND ANY REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESS OR IMPLIED, OR ANY OTHER COMMITMENT REGARDING THE CONTENTS, INCLUDING SERVICES OR PRODUCTS, DESCRIBED WITHIN THIS DOCUMENT. NOTHING IN THIS DOCUMENT MAY BE CONSTRUED OR INTERPRETED AS A BINDING COMMITMENT AND MUST NOT BE RELIED ON, INCLUDING (WITHOUT LIMITATION) IN RELATION TO PURCHASING DECISIONS. FIGURES, PERCENTAGES AND/OR OUTCOMES USED IN THIS DOCUMENT IS FOR ILLUSTRATION PURPOSES ONLY AND YOUR PURCHASE AND USE OF THE SERVICES AND/OR PRODUCTS DESCRIBED IN THIS DOCUMENT MAY PRODUCE DIFFERENT RESULTS. BEAMERY WILL NOT BE RESPONSIBLE FOR ANY LIABILITY, LOSS OR DAMAGE OF ANY KIND RESULTING FROM OR CONNECTED WITH THE USE OF THIS DOCUMENT. THIS DOCUMENT MAY CONTAIN INFORMATION DESCRIBING THIRD PARTY SERVICES OR PRODUCTS AND, UNLESS OTHERWISE STATED, BEAMERY DISCLAIMS ALL LIABILITY IN RESPECT OF THIRD PARTY SERVICES OR PRODUCTS. THIS DOCUMENT IS SUBJECT TO CHANGE, WITHOUT NOTICE, AND DECISIONS IN RELATION TO THE SAME ARE MADE BY BEAMERY IN ITS SOLE AND ABSOLUTE DISCRETION.

Beamery is, unless otherwise stated, the owner or authorized user of all copyright and other intellectual property rights. The names and logos of Beamery's partners, investors and customers are the intellectual property of the respective partner, investor or customer organisation or their affiliates, and use by Beamery does not imply endorsement or approval. No part of this document may be published, distributed or reproduced in any material form. Customers who purchase Beamery's services must make their purchasing decisions based on products, features and functionality that are currently available.

Beamery Ltd is a private limited company, incorporated in England and Wales under company number 08342136. Beamery Inc. is a corporation organised under the laws of the State of Delaware, USA with file number 5469735. Legal comments, queries or feedback in relation to this product overview can be sent to *legal@beamery.com*.