CULTURAL INTELLIGENCE CENTER

CQC Data Processing Policy

Contents

Application Overview 1
Cloud-based Processing and Security 2
- Amazon Data Centers 2
- Vulnerability Reporting, Testing and Assessments 2

Data Center Environmental Safeguards 3
- Fire Detection and Suppression 3
- Power 3
- Climate and Temperature Control 3
- Management 3

Network Security 3
- Firewalls 3
- DDoS Mitigation 4
- Spoofing and Sniffing Protections 4
- Port Scanning 4

Data Security 4
- Customer Applications 4
- Heroku Postgres 4

System Security 4
- System Configuration 4
- Customer Application Isolation 5
- System Authentication 5

Vulnerability Management 5
- Heroku Application Security 5

Backups 5
- Customer Applications 5
- Customer Postgres Databases 6
- Customer Configuration and Meta-information 6
- Heroku Platform 6

Disaster Recovery 6
- Customer Applications and Databases 6
- Heroku Platform 6

Privacy 6
Access to Customer Data 7
Employee Screening and Policies 7
Security Staff 7
Artificial Intelligence 7
User Consent 7
Data Sent for Processing 7
Use of AI Output 8
Data Retention and Model Training 8
Quality and Oversight 8
Contact Information 8
Policy Version 8

Application Overview

The Cultural Intelligence Center ("CQC") offers assessments, e-learning courses, education aids and similar products through its secure learning portal at https://cqcenter.com. This portal is built using proprietary computer code designed and developed by CQC for the purposes of delivering its products to customers around the world.

CQC customers are organizations or individuals who have contracted with CQC to provide training, consulting and information regarding Cultural Intelligence, Cultural Values, and related matters. All CQC customers voluntarily provide certain personal information for the purposes of receiving feedback, accessing e-learning course offerings, or furthering their personal development.

CQC only collects information that is provided voluntarily by our individual customers ("users") or their organizations. We do not use any of the information provided to us to make inferences about users that are used for other purposes and we do not store any information about users that is not provided to us by completing a form or an assessment. We do not share users' personal data with any third parties, except (1) when users provide permission to share with qualified University researchers, and (2) when users consent to AI-assisted personalized feedback, as described in the Artificial Intelligence section below. If individual users are students or are part of an organization that has contracted with CQC to provide training, then the student's teacher or the user's organizational trainers or administrators may have access to such things as feedback reports or group or team reports that are an essential part of our training services.

CQC does not offer advertisements on our secure learning portal. We do sometimes provide links to other websites over which we have no control and that may offer advertising or use cookies or other methods to track visitors.

Access to the CQC secure learning portal is available only through registration, which requires that users provide us with an email address, which serves as a "user ID" and is used for all external communication from the portal to users, and a password. All information from a user's browser and local device is transmitted in encrypted format to our cloud-based servers using https web security protocol (SSL Certificate issued by GlobalSign CloudSSL (SHA256) through Heroku). All evaluative user scores and comparisons are stored in

pseudonymized form (where a random ID is substituted for the user's name) in our database. The CQC secure learning portal uses cookies for authentication and for various other purposes throughout the portal.

We offer the ability for secure LTI integration with other Learning Management Systems to hand off the user credential management responsibility through pass-through functionality to the consuming application. We can either tie user generated data to a user account provided by the integrated LMS or an unidentified user data-bind for a completely anonymous experience.

A limited group of CQC administrators has access to the administrative functions of the secure learning portal, which provides access to user data, feedback reports, e-learning scores, and similar information for the purposes of trouble-shooting or assisting users with technical issues. CQC administrators access to administrative functions is controlled through the use of passwords and https encryption protocol.

CQC takes data security and privacy seriously. A senior corporate officer serves as data protection officer as well as privacy officer. In the event of any type of data breach, the affected users will be notified promptly regarding the data breach as well as what types of information were affected.

Cloud-based Processing and Security

CQC contracts with Heroku, a cloud application platform, to provide infrastructure management, scaling, security, and security auditing for the CQC secure learning portal. Heroku, in turn, uses physical infrastructure that is hosted and managed within Amazon's secure data centers and utilizes Amazon Web Services (AWS) technology. Following is more detailed information on security and data protection by Heroku and Amazon.

Amazon Data Centers

CQC leverages AWS's S3 storage service for large file storage for items such as videos, reports, and training modules. This is the only AWS service that CQC leverages directly. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

For more information on AWS's certifications or to view the actual certificates, please visit https://aws.amazon.com/compliance/iso-certified/

Vulnerability Reporting, Testing and Assessments

Heroku continually monitors for bugs and operates a bug bounty program to reward those who find and report bugs in our platform.

Third party security testing of the Heroku application is performed by independent and reputable security consulting firms. Findings from each assessment are reviewed with the assessors, risk ranked, and assigned to the responsible team.

Heroku utilizes ISO 27001 and FISMA certified data centers through Amazon's EC2 (Elastic Cloud Computing) service. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building

ingress points by professional security staff utilizing video surveillance, state-of-the-art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Amazon only provides data center access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical and electronic access to data centers by Amazon employees is logged and audited routinely.

For additional information see: https://aws.amazon.com/security

For additional information about Heroku's certifications or to see the actual certificates, please visit https://www.heroku.com/compliance

Data Center Environmental Safeguards

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.

Climate and Temperature Control

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Monitoring systems and data center personnel ensure temperature and humidity are at the appropriate levels.

Management

Data center staff monitor electrical, mechanical and life support systems and equipment so issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

For additional information see: https://aws.amazon.com/security

Network Security

Firewalls

Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on

the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.

Host-based firewalls restrict customer applications from establishing localhost connections over the loopback network interface to further isolate customer applications. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.

DDoS Mitigation

Our infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

Spoofing and Sniffing Protections

Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. Heroku utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels.

Port Scanning

Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.

Data Security

Customer Applications

Each application on the Heroku platform runs within its own isolated environment and cannot interact with other applications or areas of the system. This restrictive operating environment is designed to prevent security and stability issues. These self-contained environments isolate processes, memory, and the file system using LXC while host-based firewalls restrict applications from establishing local network connections.

For additional technical information see: https://devcenter.heroku.com/articles/dyno-isolation

Heroku Postgres

Customer data is stored in separate access-controlled databases per application. Each database requires a unique username and password that is only valid for that specific database and is unique to a single application. Customers with multiple applications and databases are assigned separate databases and accounts per application to mitigate the risk of unauthorized access between applications.

Customer connections to postgres databases require SSL encryption to ensure a high level of security and privacy.

System Security

System Configuration

System configuration and consistency is maintained through standard, up-to-date images, configuration management software, and by replacing systems with updated deployments.

Systems are deployed using up-to-date images that are updated with configuration changes and security updates before deployment. Once deployed, existing systems are decommissioned and replaced with up-to-date systems.

Customer Application Isolation

Applications on the Heroku platform run within their own isolated environment and cannot interact with other applications or areas of the system to prevent security and stability issues. These self-contained environments isolate processes, memory, and the file system while host-based firewalls restrict applications from establishing local network connections. For additional technical information see: https://devcenter.heroku.com/articles/dyno-isolation

System Authentication

Operating system access is limited to Heroku staff and requires username and key authentication. Operating systems do not allow password authentication to prevent password brute force attacks, theft, and sharing.

Vulnerability Management

Heroku's vulnerability management process is designed to remediate risks without customer interaction or impact. Heroku is notified of vulnerabilities through internal and external assessments, system patch monitoring, and third party mailing lists and services. Each vulnerability is reviewed to determine if it is applicable to Heroku's environment, ranked based on risk, and assigned to the appropriate team for resolution.

New systems are deployed with the latest updates, security fixes, and Heroku configurations and existing systems are decommissioned as customers are migrated to the new instances. This process allows Heroku to keep the environment up-to-date. Since customer applications run in isolated environments, they are unaffected by these core system updates.

To further mitigate risk, each component type is assigned to a unique network security group. These security groups are designed to only allow access to the ports and protocols required for the specific component type. For example, user applications running within an isolated dyno are denied access to the Heroku management infrastructure as each is within its own network security group and access is not allowed between the two.

Heroku Application Security

Heroku uses penetration tests, vulnerability assessments, and source code reviews to assess the security of our application, architecture, and implementation. Heroku also performs security audits as part of their service offerings. Their third party security assessments cover all areas of our platform including testing for OWASP Top 10 web application vulnerabilities and customer application isolation. Heroku works closely with external security assessors to review the security of the Heroku platform and applications and apply best practices.

Issues found in Heroku applications are risk ranked, prioritized, assigned to the responsible team for remediation, and Heroku's security team reviews each remediation plan to ensure proper resolution.

Backups

Customer Applications

Applications deployed to the Heroku platform are automatically backed up as part of the deployment process on secure, access controlled, and redundant storage. We use these

backups to deploy your application across our platform and to automatically bring your application back online in the event of an outage.

Customer Postgres Databases

Continuous Protection keeps data safe on Heroku Postgres. Every change to your data is written to write-ahead logs, which are shipped to multi-datacenter, high-durability storage. In the unlikely event of unrecoverable hardware failure, these logs can be automatically 'replayed' to recover the database to within seconds of its last known state. We also provide you with the ability to back up your database to meet your own backup and data retention requirements. For additional technical information see: https://devcenter.heroku.com/articles/pgbackups

Customer Postgres Databases are backed up both logically, as described above, and physically. Physical backups are spread across three separate servers located in the AWS server region for our application (us-west-2 in Oregon, US).

Customer Configuration and Meta-information

Your configuration and meta-information is backed up every minute to the same high-durability, redundant infrastructure used to store your database information. These frequent backups allow capturing changes made to the running application configuration added after the initial deployment.

Heroku Platform

From our instance images to our databases, each component is backed up to secure, access controlled, and redundant storage. Our platform allows for recovering databases to within seconds of the last known state, restoring system instances from standard templates, and deploying customer applications and data. In addition to standard backup practices, Heroku's infrastructure is designed to scale and be fault tolerant by automatically replacing failed instances and reducing the likelihood of needing to restore from backup.

Disaster Recovery

Customer Applications and Databases

Our platform automatically restores customer applications and Heroku Postgres databases in the case of an outage. The Heroku platform is designed to dynamically deploy applications within the Heroku cloud, monitor for failures, and recover failed platform components including customer applications and databases.

Heroku Platform

The Heroku platform is designed for stability, scaling, and inherently mitigates common issues that lead to outages while maintaining recovery capabilities. Our platform maintains redundancy to prevent single points of failure, is able to replace failed components, and utilizes multiple data centers designed for resiliency. In the case of an outage, the platform is deployed across multiple data centers using current system images and data is restored from backups. Heroku reviews platform issues to understand the root cause, impact to customers, and improve the platform and processes. The platform will auto-scale to accommodate large spikes in traffic, but caps the scaling to provide application stability across the entire Heroku platform.

Privacy

Heroku has a published privacy policy that clearly defines what data is collected and how it is used. Heroku and salesforce.com are committed to customer privacy and transparency.

We take steps to protect the privacy of our customers and protect data stored within the platform. Some of the protections inherent to Heroku's products include authentication, access controls, data transport encryption, HTTPS support for customer applications, and the ability for customers to encrypt stored data. For additional information see: https://www.heroku.com/policy/privacy

Access to Customer Data

Heroku staff does not access or interact with customer data or applications as part of normal operations. There may be cases where Heroku is requested to interact with customer data or applications at the request of the customer for support purposes or where required by law. Customer data is access controlled and all access by Heroku staff is accompanied by customer approval or government mandate, reason for access, actions taken by staff, and support start and end time.

Employee Screening and Policies

As a condition of employment all Heroku and salesforce.com employees undergo preemployment background checks and agree to company policies including security and acceptable use policies.

Security Staff

Our security team is led by the Chief Information Security officer (CISO) and includes staff responsible for application and information security. The security team works closely with the entire Heroku organization and customers to address risk and continue Heroku's commitment to trust.

Artificial Intelligence

CQC offers optional AI-assisted personalized feedback within certain CQ® assessment reports. This feature uses Claude, a large language model provided by Anthropic, PBC, accessed through Anthropic's commercial API. Anthropic processes this data on CQC's behalf as a data processor under [Anthropic's Commercial Terms of Service and Data Processing Addendum].

User Consent

AI-assisted feedback is used only for users who give explicit consent. Consent is never pre-selected. Users who decline still receive their full report, with standard written content in place of AI-generated commentary. Users may withdraw consent at any time, after which no further information is sent for AI processing. We record each consent decision along with the version of the consent language the user agreed to.

Data Sent for Processing

Only two types of information are sent to Anthropic: the user's percentile scores and their answers to the optional background questions. Names, email addresses, and other direct identifiers are never included, consistent with the pseudonymized form in which we store evaluative scores. All data is transmitted

in encrypted format over HTTPS. Users are advised not to include names or other identifying details in their background answers.

Use of AI Output

AI-generated feedback is used only to help users connect their results to their own role and context. It does not make decisions about users and does not affect scores, certification, or any employment-related outcome. Reports containing AI-generated content are clearly labeled as such.

Data Retention and Model Training

Under Anthropic's commercial terms, data sent through the API is not used to train Anthropic's models. Inputs and outputs are retained by Anthropic for up to 30 days for trust and safety purposes and then deleted. AI-generated feedback is stored with the user's report in our database under the same protections described elsewhere in this policy.

Quality and Oversight

CQC designs and maintains the instructions that guide the AI's feedback and regularly reviews AI output against a defined quality standard for accuracy, tone, and appropriateness.

For more information on Anthropic's security practices and certifications, see https://trust.anthropic.com

Contact Information

Questions about this policy, CQC's data practices, or requests regarding personal data (including access, correction, deletion, or withdrawal of consent) may be directed to:

Brandon Gamble, Director of IT and Software Development, Data Protection Officer
Cultural Intelligence Center, LLC
29777 Telegraph Rd Suite 4200
Southfield, MI 48034
privacy@culturalq.com

Policy Version

Version 1.3, effective 11/10/2020. Last updated 10/07/2026.