



Huddle

Security / Technical Specifications



Information Hotline

0871 7000 170
+44 (0)1452 546742
conferencing@intercalleurope.com

Reservations

0870 043 4167
+44 (0)1452 553456
resv@intercalleurope.com

www.intercalleurope.com

Huddle offered by InterCall is a fully hosted product with no required software downloads. Huddle supports Internet Explorer 6 and 7, Firefox 3 and Safari 3 Internet browsers.

HOSTING ENVIRONMENT

Huddle's production systems are hosted by Rackspace in some of the most highly specified data centres available today, built to exacting, rigorous standards and delivering unparalleled security, power, connectivity and environmental control.

Rackspace provides the world-class infrastructure necessary to keep Huddle's servers up and running uninterrupted around the clock. Rackspace has several data centres in London, UK, all of which are engineered with fully redundant connectivity, power and HVAC to avoid any single point of failure. Each data centre is staffed 24 x 7 by highly trained technical support staff.

PHYSICAL SECURITY

Public access to Rackspace data centres is strictly forbidden. They only host equipment that they own and manage themselves, obviating the need for anyone but their highly trained Rackspace Engineers to be allowed into the data centre.

In addition, Rackspace employs a series of physical security measures, including:

- + Live video surveillance of each data centre facility, monitored 24 hours per day.
- + Onsite security personnel monitor each site 24 hours per day.
- + Biometric hand scanners restrict access to each data centre.
- + A pass card system restricts movement from room to room within each data centre.

Rackspace data centres are unmarked to help maintain a low profile, and these physical security measures are audited by an independent company.

SYSTEM SECURITY

Our servers run a hardened OS, with security patches applied by Rackspace to provide ongoing protection from exploits. Network level security is provided by dedicated Cisco firewalls, together with DDoS mitigation provided by Rackspace's proprietary Rackspace PrevenTier system. Huddle's application infrastructure has undergone thorough independent penetration testing, which found no security vulnerabilities.

Rackspace operational policies and procedures are based on ISO17799, and regularly reviewed as part of their SAS70 Type II audit. All system access is fully logged and tracked for auditing purposes, and all staff with access undergo a thorough background check.

APPLICATION SECURITY

When accessing any paid-for account on Huddle, Secure Socket Layer (SSL) protects your user name and password information by providing both server authentication and 128-bit AES data encryption. This ensures that your data is safe, secure, and available only to registered users in your organisation.

Huddle requires that each user has a unique user name and password that must be entered each time a user logs on. Huddle issues a session cookie only to record encrypted authentication information for the duration of a specific session. The session cookie does not include the user name or password, or any user data, and it is deleted when the browser is closed.

Huddle application security ensures that only those invited in to a workspace can access its contents. Access controls are baked in to the Huddle data model, and user permissions are verified on every request by the core Huddle application framework.

These access controls apply not only at the workspace level, but can also be applied to specific file folders to restrict access to certain workspace members. Access can be provided as either "read only" or "edit".



The Huddle application has been rigorously tested against common website vulnerabilities such as cross-site scripting (XSS), cross-site request forgery (XSRF) and SQL injection.

UPTIME & RESILIENCE

At Huddle we recognise that uptime is of the up most importance for a business-critical web application. We employ two separate external monitoring systems to track and record availability and response time from various locations around the globe. We have a 24x7 team available to respond in the unlikely event of a serious application issue.

Huddle's Service Level Agreement guarantees uptime of 99.5% every month. Our record shows we are always performing well above this SLA: for example in 2009 Huddle's application was available 99.96% of the time.

Huddle's excellent uptime is achieved by planning in redundancy in every part of the system, coupled with careful quality assurance and change management. This redundancy applies to everything from power and network connections in to Rackspace data centres, firewalls, load balancers, switches, web servers, database servers. Each server has redundant NICs, and all hard drives are configured in RAID 1 or RAID 5 arrays with a hot spare.

BACKUP & DISASTER RECOVERY

All of Huddle's servers are backed up nightly, and backups are retained for two weeks. In addition, all data (database and file system) is mirrored almost immediately to standby servers in a second UK data centre. This second data centre deployment is likewise backed up nightly and backups are retained for two weeks.

In the event of the most serious of catastrophes resulting in the complete loss of our primary data centre, workspaces belonging to paid-for accounts will be available within a matter of minutes via our Disaster Recovery site. Data is replicated to this site in near real-time, so business as usual can proceed seamlessly.

AND HERE'S WHAT CUSTOMERS HAVE SAID

"QIA (UK Government Agency) ways of working have certainly improved since the adoption of Huddle. Being a commissioning organisation, our communication and document management practices with our contractors are much more effective, thanks to this central document repository.

The security technology behind the application and the easy permissions settings also allow us to share confidential information and personal data without worrying about them falling in the wrong hands. This has helped us meeting some of our legal requirements in terms of Data Protection and Information Security."