

## Hosting and security

# Learn about how we protect your data

## 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. Huddle hosts in two UK data centres, both of which are engineered with fully redundant connectivity, power and HVAC to avoid any single point of failure.

## 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 IDS and DDoS mitigation provided by Rackspace. Huddle's application infrastructure is subject to regular independent penetration testing – as part of our PCI-DSS compliance.

Rackspace have ISO27001 certification for their operational policies and procedures, are they are 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 in line with UK Government standards.

## APPLICATION SECURITY

When accessing any paid-for account on Huddle, Secure Socket Layer (SSL) is used across the entire site to encrypt all data exchanged with the server to industry standard levels, as well as authenticating the server itself to the user.

Huddle provides each user with 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 correct operation of all security controls is confirmed by a set of automated tests before every new release of the Huddle application.

Huddle has been rigorously tested against web application vulnerabilities such as cross-site scripting (XSS), cross-site request forgery (XSRF) and SQL injection, with a number of our customers also commissioning their own independent testing, including manual ethical hacking.

UK Government departments have also performed their own inspections of Huddle's office environment, processes, and hosting facilities in order to ensure that they can rely on our security measures.

## UPTIME & RESILIENCE

At Huddle we recognise that uptime is of the upmost 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 99.9% every any 3 month period. Our record shows we are always performing well above this SLA: for example in Q1 of 2010 Huddle's application was available 99.99% 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, through to clustered web servers and database servers.

## 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. Files deleted from Huddle Enterprise or Professional workspaces are retained for 90 days to allow recovery following accidental deletion. They are permanently deleted at the end of this 90 day period.

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.