Enterprise level security, the Huddle way.
# Security whitepaper

## TABLE OF CONTENTS

1. Huddle’s promise
2. Hosting environment
3. Network infrastructure
4. Multiple levels of security
   - Physical security
   - System & network security
   - Application security
5. SLA & resilience
6. Backup & data recovery
7. Privacy
8. Considerations on the software lifecycle
9. FAQ
   - Security
   - Privacy
10. About Huddle
HUDDLE’S PROMISE
Huddle is committed to keeping your data safe and secure. Some of the biggest businesses in the world, and numerous government organizations, trust Huddle with their data. This document will give you an overview of Huddle’s secure infrastructure and policies. You will also find some FAQs at the end of the document. Should you have any further questions regarding our security policies and measures, please don’t hesitate to get in touch with us.

HOSTING ENVIRONMENT
Huddle’s production systems are hosted by Rackspace in some of the most highly specified data centers available today. They are built to exacting, rigorous standards and deliver 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 highly secure data centers 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 24/7 by highly trained technical support staff. Huddle has selected to host it’s data in the UK to ensure that it is protected by EU data laws.

NETWORK INFRASTRUCTURE
The following diagram illustrates Huddle’s primary and disaster recovery infrastructure.
MULTIPLE LEVELS OF SECURITY
Huddle has implemented security on multiple levels to offer the maximum level of protection to its customers’ data. The following paragraphs describe each level in more detail.

PHYSICAL SECURITY
Public access to Rackspace data centers is strictly forbidden. The organization only hosts equipment that it owns and manages, obviating the need for anyone but its highly trained Rackspace Engineers to be allowed into the data center.
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 center
• A pass card system restricts movement from room to room within each data center

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

SYSTEM & NETWORK 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.

Rackspace’s operational policies and procedures are regularly reviewed as part of its SAS 70 Type II audit, and its data center is ISO 27001 certified. All system access is fully logged and tracked for auditing purposes and all staff with access undergo a thorough background check. Servers are hosted behind sophisticated firewalls, with a protected perimeter. We carry out penetration testing on an ongoing basis and have had formal penetration testing commissioned on a number of occasions by third parties.

APPLICATION SECURITY
All access to Huddle is protected by Secure Socket Layer (SSL) providing both server authentication and 256-bit AES data encryption. This ensures that your data is safe, secure and available only to registered users in your organization, with relevant permissions.

Huddle provides each user with a unique username 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 username, password, or any user data. Huddle’s password control includes a strength indicator and protection against brute-force attempts to discover passwords.

Huddle’s 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”, “edit” or “no access”.

Huddle is able to offer IP address locking, meaning you can lock access to Huddle as a whole, or certain workspaces only, to individual IP addresses (i.e. specific computers or office locations).

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.
SLA & RESILIENCE
At Huddle, we recognize 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 (SLA) guarantees uptime of 99.9 per cent over any three month period. Our record shows we are always performing well above this SLA. For example, in the first six months of 2011, Huddle’s application was available 99.99 per cent of the time. Our performance against our SLA is publicly available in real-time from a third-party who monitor our service (Aware Monitoring).

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.

BACKUP & DISASTER RECOVERY
To minimize service interruption due to hardware failure, natural disaster, or other catastrophes, Huddle implements a disaster recovery program. 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.

In the event of the most serious of catastrophes, resulting in the complete loss of our primary data centre, workspaces belonging to paying 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 can proceed as usual.

PRIVACY
Huddle maintains a strong privacy policy to protect customer data. Huddle does not own customer data or share it with third parties. Huddle also allows customers to take their data with them, should they decide to stop using Huddle’s services. The full privacy policy is available upon request.

CONSIDERATIONS ON THE SOFTWARE LIFECYCLE
Huddle employs an Agile development methodology, using Scrum alongside selected Extreme Programming (XP) practices. This iterative approach to development ensures that Huddle can release incremental product enhancements on a very frequent basis, and modify the product plan quickly and easily in response to changing priorities.

Each development iteration lasts two weeks. This includes all the planning, design, development and exhaustive quality assurance activities to ensure that the output is production ready, following a short but rigorous regression testing process the majority of which is automated.

Once the Quality Assurance team have approved the product increment for deployment to the live environment, the Systems Engineering team performs the release. Releases typically take place every four weeks and the dates are published in advance. Standard releases do not involve any application downtime.
FAQ

SECURITY

Where is my organization’s data stored?
All customer data is stored in Rackspace data centers, in the UK. More information on these data centers is available upon request.

How do you protect your infrastructure against hackers and other threats?
Servers are hosted behind sophisticated firewalls, with a protected perimeter. We carry out penetration testing on a regular basis and have had formal penetration testing commissioned on a number of occasions by third parties. Our customers are welcome to carry out their own penetration testing by prior arrangement with Huddle.

How do you protect from machine downtime?
Huddle has a complete disaster recovery plan which makes use of failover to our second data center. This is kept up to date in real time. The worst case scenario for physical disaster at our primary data center has a 15 minute failover time to the second data center.

This redundancy is built into each application layer of the Huddle platform. Huddle as a business runs entirely on cloud based services and our business continuity plan reflects this. Our service is designed to continue running even in the event of a major incident at our business premises. All Huddle staff are provisioned with the tools required to work remotely in the event of a major disaster.

Does Huddle offer SSL connectivity?
All data on Huddle is fully encrypted with 256-bit SSL encryption.

PRIVACY

Who owns the data that my organization stores on Huddle’s servers?
All the data on Huddle’s server belongs to the customer and it can extracted upon request, should this be necessary.

Does Huddle give third party access to my data?
Huddle does not give third parties access to its customers’ data and it enforces a strict privacy policy.

Does Huddle have a Safe Harbor certification?
“Safe Harbor” is a framework developed by the US Department of Commerce in consultation with the European Commission to bridge the differences between the EU and US privacy policy. It allows US companies to comply with the EU’s more rigorous data protection law.

Since Huddle is a UK company, and all customer data resides in the UK, it is protected by the EU Data Protection Direction, which is regarded as one of the most rigorous Privacy legislations in the world and does not need Safe Harbor certification. Contact us to have more information on Huddle’s privacy policy.

Is my data subject to the Patriot act?
The Patriot Act, passed in 2001 by the US, that any US company or wholly-owned subsidiary of a US company must hand over data that they are hosting on behalf of their customers if they are requested to do so by the US authorities. What this means in reality is that, if you are buying a cloud-based service from a US company, your data can be made available to US authorities upon request without your permission. Huddle is a UK company and we use UK-based hosting providers so we can guarantee that any data we host on behalf of our customers is not subject to the Patriot Act.
Can I extract my data should we wish to archive?

Huddle can provide a data export tool which allows all information stored within Huddle to be exported to a local system of your choosing (e.g. network drive/personal hard drive etc.) This includes:

- All documents extracted to a standard file and folder format
- All web based information (e.g. discussions/whiteboards) in offline HTML format
- Tasks - by workspace export

It is also possible to run this on a scheduled basis, so that the risk of loss of information is doubly mitigated (bearing in mind that Huddle already runs industry leading datacentre mirroring and disaster recovery on your behalf).

ABOUT HUDDLE

Established in November 2006 and based in London and San Francisco, Huddle is the leader in Enterprise Collaboration and Content Management in the cloud.

With Huddle, you can manage projects, share files and collaborate with people inside and outside of your organization, securely. It is available online, on mobile devices, on the desktop, via Microsoft Office applications, major business social networks and in multiple languages. Simply: if SharePoint was built today, they would have built Huddle.