Ideagen Huddle

Information Security Overview

Ideagen
Huddle™

Contents

1. Introduction

Huddle has provided cloud collaboration solutions to global enterprises, governments, and public sector organizations since 2006.

To be a trusted cloud provider, Ideagen Huddle understands that today's organizations require an exceptionally high standard of security without compromising ease of use or functionality. Governments and enterprises require their documents and content to be stored securely so that they can be made available to their employees, partners, and stakeholders in real-time. No matter what device you use or where you are geographically, you want to be able to rest assured in the knowledge that what your team have entrusted to Huddle remains available, secure, and intact. That's why maintaining the highest level of confidentiality, integrity and availability of our customers' data and information is one of the guiding principles of information security at Huddle.

Our services are audited by accredited third party organizations to ensure we meet the required industry standards. Additionally, our approach to ISO/IEC 27001:2013, Cyber Essentials Plus, FedRAMP and other certifications are designed holistically, allowing us to introduce a foundation which is sufficiently flexible to allow the adoption of other certifications, best practices, regulatory and compliance standards.

Huddle invests considerable time and resource into its strategies and security team whose key focus includes information security, compliance, and risk management, all to help you advise your company board, management teams, employees, and clients.

Information security is driven by the board through the management hierarchy, and within Huddle through a security program that ensures knowledge and best practice is spread across all departments of the business. Effective information security requires continual improvement to established and accepted practices from across the ecosystem. Benchmarking against ISO/IEC 27001:2013 and other frameworks gives us the ability to properly maintain and improve processes, policies, and audit functions. This ensure Huddle's information security is at the forefront of best practice.

Huddle's products are protected by several commercial, proprietary, open source and internally authored systems.

Countermeasures are in place to protect you against evolving cyber threats and risks, including (but not limited to):

- Man-in the-middle
- Malware
- Session hijacking
- Cross-site scripting (XSS)
- Cross-site Request Forgery (XSRF)
- SQL Injection
- Denial of Service (DoS)

2. Security principles

CLOUD SECURITY PRINCIPLE	WHAT HUDDLE DOES
DATA IN TRANSIT PROTECTION	Huddle protects all data in transit with the FIPS 140-2 compliant TLS 1.2 protocol which utilizes strong ciphers and 256-bit key lengths.
ASSET PROTECTION & RESILIENCE	Huddle has partnered with an industry leading infrastructure provider AWS, who have adopted SOC1, SOC2, SOC3, and industry best practices for the physical protection of information processing assets. Your file content is protected by FIPS 140-2 and is 256-bit AES data-at-rest encryption compliant. ISO/IEC 27001:2013 certified policies and processes ensure that all endeavors to protect information assets have been verified and audited by URS, a globally recognized body for standards.
SEPARATION BETWEEN USERS	Huddle's services are multi-tiered and multi-tenanted. The use of stringent industry best practices and business logic ensures that information isn't unintentionally disclosed between Huddle clients. The confidentiality, privacy and ownership of information is always maintained and access to content must be explicitly granted by you, the customer.
GOVERNANCE FRAMEWORK	Huddle's global information Security Management System (ISMS), which incorporates the protection of information security assets, is verified by URS for adherence to the ISO/IEC 27001:2103 standard. Huddle's U.S. instance is FedRAMP Moderate approved and audited by Coalfire Systems Inc.
OPERATIONAL SECURITY	Huddle's global services are monitored and managed via continuous improvement methodologies that allow for the review of current security policies and procedures. Huddle reviews its information security policies and procedures annually through the 'Plan, Do, Check, Act' cycle.
PERSONNEL SECURITY	Huddle Global Instance: Ideagen, who own the Huddle product, conduct background checks by requesting two previous employment references. An employment offer with Ideagen is conditional on receipt of satisfactory references. Roles for more senior positions may be subject to full disclosure background checks conducted by a third party. Huddle FedRAMP Instance: All Ideagen Huddle employees are screened prior to employment with the following checks: • Six-year address history • Right to work in the United Kingdom, United States of America, or South Africa • Three years of employment history • Education Verification • Criminal (federal, state, county), unspent convictions, DMV (motor vehicles) and SSN matching Huddle employees with authorized access to production and test environments are screened prior to access being granted. These employees undergo pre-employment screening using an external service that follows the BS 7858:2019 standard and attend production access training annually.

CLOUD SECURITY PRINCIPLE	WHAT HUDDLE DOES
SECURE DEVELOPMENT	Huddle has information security built into the heart of the Software Development Lifecycle (SDLC) policy and process. Huddle's services are developed with stringent 'OWASP Web and Mobile Top-10'-derived industry-standard practices.
SUPPLY CHAIN SECURITY	All of Huddle's suppliers are subject to a rigorous due diligence process to ensure that their security management controls policies and processes are commensurate with Huddle's.
SECURE USER MANAGEMENT	Huddle provides rich management functionality allowing companies and their departments to adhere to security requirements. For example: access control, auditing and usage logging, creation and deletion of users. Huddle also provides rich security-centric functionality such as mobile application PIN, view-only content, access permissions, and native two-factor authentication.
IDENTITY & AUTHENTICATION	Web browser and device access to Huddle is secured and authenticated by the industry-standard OAuth 2.0. Single sign-on (SSO) via SAML, allowing you to have greater control over access granularity, authentication, and identity management.
HOSTING PROVIDERS / EXTERNAL INTERFACE PROTECTION	We have partnered with an industry leader in IaaS hosting who have well-established governance programs in place. They adhere to the most stringent security management methodologies and standards; ISO/IEC9001, ISO/IEC 27001:2013, FedRAMP, SOC 1, 2 and 3.
SECURE SERVICE ADMINISTRATION	We are governed by infrastructure management policies and processes which include the utilization of industry-standard practices that govern Change and Operational Management. The governance we practice ensures the confidentiality, integrity, and availability of your content.
AUDIT INFORMATION FOR USERS	Huddle provides end-user and administrative reports that detail usage and access to all content stored in its services.
SECURE USE OF THE SERVICE	You are provided with the knowledge of how to best implement and manage the product to ensure all your content remains accessible and available on a need-to-know basis. This is achieved through the utilization of: • Customer Success Managers • An extensive online knowledge base • Instructional usage videos • Ticket based support portal

3. Huddle in government

HM Government G-Cloud Supplier

FedRAMP™

UK (G-Cloud)

Huddle is widely used in UK Government and their broader ecosystem. It is available via the G-Cloud Digital Marketplace and offers a variety of services tailored to market requirements.

We were one of the first cloud service providers to be awarded Pan Government Accreditation (PGA) by CESG (GCHQ) under the previous Impact Level classification and are certified with Cyber Essentials Plus. The platform is also security tested against the Information Technology Health Check (ITHC) standards as evidenced through the annual ITHC compliant penetration test.

The platform adheres to all 14 National Cyber Security Centre (NCSC) Cloud Security Principles , which details how cloud providers should manage the services advertised on G-Cloud. Several UK Public Sector Senior Information Risk Owners (SIRO) have assessed and entrusted the use of Huddle for Official (OFFICIAL-SENSITIVE) content.

U.S. (FedRAMP)

Huddle was one of the first SaaS providers to achieve a 'FedRAMP Authority to Operate (ATO)' and was also the first cloud-based collaboration company to achieve this status. With a commitment to meet stringent U.S. Government security requirements, Huddle has a separate instance of Huddle with data centers located in the U.S. to meet the needs of U.S. government departments.

4. Huddle's hosting partners and governance

Amazon Web Services (AWS)

As one of the leading providers of cloud services globally, Amazon's services provide a fabric for Huddle to build scalable, performant, and secure services for the benefit of Huddle customers.

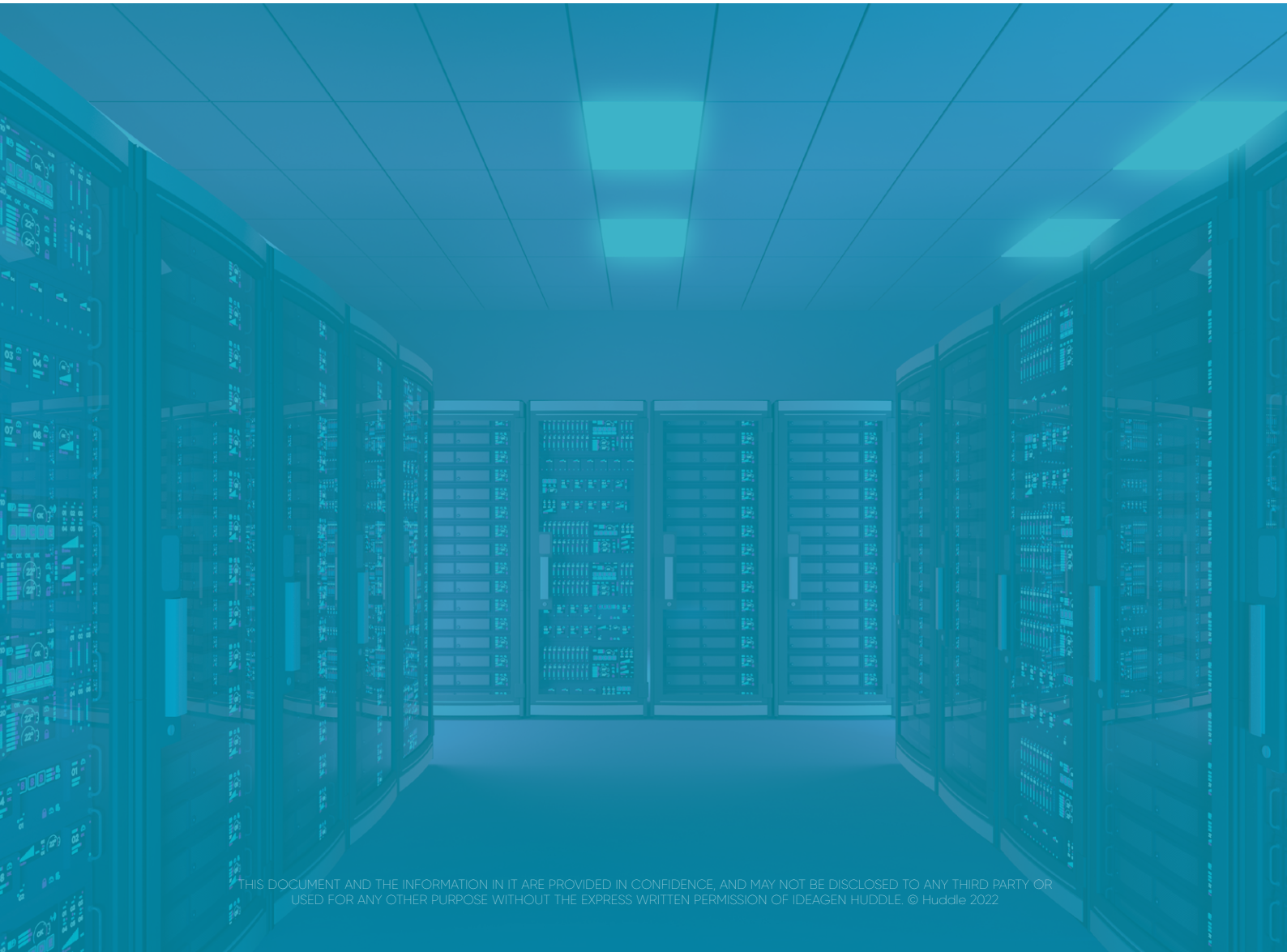
Datacenter access control

All our Huddle data centers are compliant and certified to the highest standards, therefore, the physical and logical access control is an exceptionally vital component of this. Ensuring that the right people have the right clearance removes significant risk from interruption of service, corruption of content and accidental or intended disclosure of content and documents. Huddle has exceptionally stringent Access Control policies based on industry best practice.

Data Residency

We have two territories where Huddle customer content can reside: the UK and the US.

There is a separate instance of Huddle in each location. Each territory has different legal requirements and interconnectivity agreements in place to ensure that content benefits from the country-specific protections in which it's hosted. We have implemented multiple availability zones in region to ensure continuity of service through real-time replication.



5. Certifications, standards, and accreditations

Huddle has a long history of security, and we work hard to build trusted relationships with our clients. Not only were we one of the first cloud collaboration providers to achieve government accreditation in both the UK and the US, but we continue to invest in meeting the requirements of many of the industry's most widely recognized security standards, including ISO/IEC 27001:2013, Cyber Essentials Plus and FedRAMP.

ISO/IEC 27001:2013

At the heart of ISO/IEC 27001:2013 is the Information Security Management System (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical, and technical controls involved in managing sensitive and secure information through risk-management based policies and processes. The specification includes details for documentation, management responsibility, internal audits, continual improvement, and corrective and preventive action. The standard requires cooperation among all sections of an organization. Huddle is independently audited by a third-party and certified by United Registrar of Systems (URS) - a trusted partner recognized in audit and certification worldwide.

Cyber Essentials Plus

Cyber Essentials Plus is a third-party, independently audited, annual certification which supports the UK Government's National Cyber Security Strategy.

Managed by the Information Assurance for Small and Medium Enterprises Consortium (IASME), meanings barriers, such as cost, faced by smaller organizations are reduced significantly. It also gives SME's a legitimate way to show that they are compliant and have taken steps to protect their client and partner data.

The audit focuses on five technical control themes:

- Firewalls
- Secure Configuration
- User Access Control
- Malware Protection
- Patch Management

Six Degrees, an IASME accredited certification body, completed Ideagen Huddle's assessment; the scope of which includes Huddle's company systems, policies, processes, and any third-party services that store confidential content.

FedRAMP

FedRAMP is a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Based on our ISO/IEC 27001:2013 certificate, Huddle has demonstrated its commitment to the NIST 800-53 rev 4 System Security Plan (SSP), its 17 control families and 325 individual controls. Huddle's SSP is independently assessed by CoalFire Systems Inc who are also an approved FedRAMP Third Party Assessment Organization (3PAO).

Huddle hosting provider accreditations

We chose Huddle's hosting provider with security in mind. Our provider adheres to unique certifications specific to data centers, including a combination of:

- PCI DSS Level 1
- SOC 1
- SOC 2
- SOC 3
- ISO/IEC 27001:2013
- ISO 27017:2015
- ISO 9001:2015
- Cyber Essentials +
- HITRUST
- G-Cloud
- FedRAMP (Moderate)
- Compliant with Information Technology Infrastructure Library (ITIL) IT Service Management standards.

Privacy

Ideagen Huddle Ltd - trading as Huddle - take data privacy and protection very seriously. The General Data Protection Regulation (GDPR) came into effect in May 2018 and Huddle is fully compliant with the regulator - both as Data Controller of Personal data, which we collect and use for our own purposes, and as a Data Processor for Personal Data, which we receive from our customers as part of the service we offer. Huddle also conforms with DPA 2018 guidelines. How Huddle use data is outlined in our Privacy Policy.

Huddle has been registered as a Data Controller with the Information Commissioners Office since 2007 (Data Protection Register Number: **Z9592961**).

6. Technical engineering

Secure system development lifecycle

All roles within Huddle are clearly defined. Access to resources and environments is granted by requirement of a role only. Segregation of environments is managed both by policy and by technologies such as ACLs and firewalls. These restrictions and safeguards are in place to ensure only those personnel and systems that need access receive the appropriate level of access to complete the task - utilizing the principle of 'Least Privilege' as per industry best practice.

Policies and processes ensure employees are capable of being effective and efficient without increasing the risk of 'insider threat', configuration drift, data leakage or the stability of Huddle's services and business operations.

Test and development environments are separated so that stored production content is never removed from segregated and secured production systems. The controls in place to secure customers' content and meta-content such as: username, personal details, profile information and usage audit, always protect this data. These controls include environment, change management, access control and redundancy.

Testing & quality

We develop all software and services following a swift methodology based on AGILE. The System Development Lifecycle (SDLC) includes the OWASP Top Ten - a powerful awareness document for web application security. The OWASP Top Ten is industry-recognized and an industry-led list that represents the most recently known critical web application security flaws. This allows our Quality Assurance team to conduct extensive functionality testing prior to release.

To reduce the risk of bugs in the Huddle system, we implement automated testing, incorporating: unit, integration, end-to-end tests, continuous integration and constantly release new code for development and test environments.

These tests include, but are not limited to, malicious user input, static and dynamic code scanning, confirming all resources require authorization, XSS & XSRF/CSRF testing, session management, secure/insecure direct object references and functional access control.

Independent security consultancy & penetration testing

Six Degrees are Huddle's partner for security consultancy and penetration testing on Huddle's Global instance. Their credentials include CREST membership, and they are a CESG CHECK. Six Degrees provide independent testing and a review of all Huddle infrastructure and services on the Global instance. This ensures that we have an 'outside' perspective of how effectively implemented our security policies and processes are.

Six Degrees completes, at a minimum, an annual full global IT Health Check which is ITHC compliant. They also perform a holistic penetration test on all Huddle assets pertaining to the Global instance of Huddle. This allows us to gain insight into Huddle's security posture.

Coalfire have partnered with us to provide security consultancy and penetration testing on our US instance of Huddle. They provide independent testing and reviews of all Huddle US infrastructure and services. They complete an annual global holistic penetration test on Huddle's US assets.

The scope of these engagements include: all infrastructure hosting partners, Huddle's international offices and associated WAN as well as desktop and mobile software supplied by Huddle.

Vulnerability & Patch management

All business operations and Huddle service infrastructure are scanned for vulnerabilities, security patch levels and potential configuration issues via specialized commercial solutions. This incorporates daily changes to the database of new threats and vulnerabilities, enabling Huddle to quickly mitigate and reduce the risk of exploitation by known methods.

Our strategy and policy governing the management and control of vulnerabilities adheres to industry standards, is certified to ISO/IEC 27001:2013, and complies with FedRAMP Moderate's continuous monitoring processes and timelines.

Monitoring

Huddle has exceptionally detailed auditing in both Huddle applications and the underlying infrastructure, hardware, operating systems and network devices. Escalation of reported threats is managed by our 24/7 Technical Operations team. Huddle's Incident Response policy and process are certified to ISO/IEC 27001:2013 and FedRAMP Moderate controls which ensures a fluid, efficient, yet forensic level of detail investigation. This includes triaging priorities, threats, and a process for remediation.

We utilize SaaS providers NodePing and New Relic to ensure integrity and availability independent of the service's internal monitoring.

Configuration management

Huddle goes through initial and continual hardening of all its business operations and service infrastructure.

This ensures that Huddle has a risk and threat adverse baseline configuration, meeting and exceeding industry and Center for Internet Security (CIS) standards.

Service integrity & resilience

Huddle's chosen cloud services provider, AWS operate on a 5 9's principle of uptime. The services can account for multiple core components failures whilst remaining available to customers. In the unlikely event that a data center was to fail, Huddle has multi-geo located data centers to ensure the continuity of service. Huddle's Service Level Agreement) (SLA) will start service credits if service uptime drops below 99.7% We are able to provide reports generated from NodePing and New Relic upon request.

Transport security

Huddle meets industry best practices exclusively using TLS 1.2 on all Huddle services.

All public internet accessible certificates are signed with RSA 2048-bit keys. The signature algorithm used is SHA 256 (with RSA) and Huddle utilizes Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL), ensuring the certificates utilized by customers are meeting accepted industry standards.

Huddle maintains a chain of trust for the encryption of content transportation, from our Huddle's service to all customers. The entire certificate chain, from our Certificate Authority and intermediate certificate to Huddle's issued certificate, are maintained and monitored to the same standards.

Encryption within the environment

Data at Rest Encryption is enabled for all customers, ensuring additional security on their content that is stored within Huddle's services. Content storage is protected by FIPS 140-2 compliant 256-Bit AES - the accepted industry standard for content encryption.

Huddle never store passwords in clear text. A hash of the password is 'salted' when setting or resetting to ensure additional protection. Devices and integrations utilize authorized OAuth 2.0 tokens to gain access to content. Key management strictly adheres to established and mature internal policies, in the FIPS 140-2 and FedRAMP Moderate controls.

Data loss prevention

Huddle's services are open standards-based, built on industry standard protocols and connectivity. Application Program Interfaces (APIs) enable deep integration with already established internal, external and cloud based DLP solutions. The rich functionality that the APIs provide ensures that Huddle is capable of meeting current and future requirements - protecting the distribution and access to your content within the Huddle platform.

7. Platform security

Administration access

All of Huddle's services share the same rich, functional, tiered access and control methodology. This ensures that regardless of endpoint (web, mobile or integration), there is consistent access and user interaction with a standard but simple management workflow.

Huddle's administrative access is purposefully built to quickly grant or remove users access, lower or increase privileges, customize access and sharing policies to adhere to your corporate policies. The administrative access further provides an audit of changes made to the account.

Authentication & access

Huddle's services have an industry-accepted native password policy:

- At least eight characters long
- A mix of upper and lowercase
- Includes at least one number
- Includes at least one special character e.g.!@#?%

If a user tries to log in unsuccessfully ten consecutive times, the user will be locked out for a brief period to mitigate against automated brute force attacks on the account.

If a user does not perform an action within a (configurable) set period, Huddle will automatically log the user out from the service to ensure confidentiality of the content.

Huddle customers who require more restrictive authentication and access policies can utilize Huddle's Security Assertion Markup Language (SAML) functionality.

This enables Single-Sign-On (SSO) integration across Huddle's services, as well as the adoption of already established client password complexity policies, including multi-factor authentication solutions. Huddle has partnered with some of the leading Authentication as a Service (AaaS) providers to ensure secure and functional integration.

To limit the risk of data leakage, Huddle can limit collaboration on files and content to specific email domains. With this functionality, company managers can restrict access to individual email addresses or entire domains e.g., all users with a @huddle.com, or john.smith@huddle.com only.

Organizations can finely tune access control within Huddle to harmonize with already established internal policies.

Granting and managing user access to your content

Huddle uses a Workspace model for granting and managing access to content. Workspaces are logical groupings of content managed by a Workspace manager. The Workspace manager can add/remove users and grant the necessary permissions.

Individual users are members of an Account. Additionally, users can be placed in Teams that enable further access and permission controls.

There are several ways to get users collaborating in Huddle. These include:

- On-demand user creation through SAML functionality provided by your Identity Provider (IdP) or Active Directory Federations Services (ADFS).
- Email an invitation to those you want to collaborate with. The process includes a unique single-use link that is sent directly to the user. If they are already Huddle users, they will be granted access instantly, if not they will be required to complete a light and short 'account creation' procedure.
- Huddle's Customer Success team can create accounts and associated workspaces as part of the on-boarding process for new customers.

Content stored in Huddle can have Read-Only, Read & Write or No Access permissions set for

users or teams. Users denied access cannot see folders without granted permissions, ensuring the confidentiality of that data. Our permissions-based methodology is easy to understand and can be adopted quickly across all Huddle services.

Mobile access and management

Huddle content can be accessed via native iOS and Android devices. Access to Huddle's services is granted via the industry-standard OAuth 2.0 protocol. Deployment of mobile endpoints and applications can be managed via Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) providers such as VMware, MobileIron and IBM.

These services allow for the granular management of end-user devices and applications to ensure that access to restricted and management controls adhere to your company's already established policies.

Audit & usage

Huddle's services have integrated audit functionality that includes content access, update, creation/ deletion, and permissions. Additional, and more granular, reporting can be published on request via the Huddle Customer Success Team. The level of reporting available ensures quick and easy adherence to your already established audit policies.

About Ideagen Huddle

Ideagen Huddle empowers confident collaboration across internal teams and external partners. The cloud-based solution makes it easy for teams to stay productive whilst working securely beyond the firewall.

As a leader in collaborative technology and trusted by companies around the world, Huddle helps your teams come together on all your projects. We make it easy for teams, stakeholders, and your clients to collaborate on projects, share and edit files, assign tasks, and track team activity in a secure, cloud-based environment.

Make Huddle your solution of choice.

Find out more

Ideagen Huddle™