

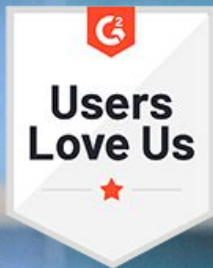


Hub Security

Software That Gets The Thumbs Up.

hub.pancentric.com





Users
Love Us



The Hub is a key communication tool for supporting our growing business. It's an easy 'off-the-shelf' solution to start up a group intranet to get colleagues quickly engaged.

The best thing is the intuitive design that is quick and easy to develop to meet our business needs.

The Hub helps us knits together recent acquisitions into our group culture, making all colleagues feel part of our wider Group business, shared objectives and ambitions.

Tom Storer
Group Operations Director



Contents

Hub Security At A Glance

[4](#)

Industry Recognised Solution

[5](#)

Hub Security:

- **Infrastructure Security**

[7](#)

- **Software Security**

[8](#)

- **Product Security**

[9](#)

- **Custom Password Policy**

[10](#)

- **Data Protection & Privacy**

[11](#)

- **Company Processes & Security Policies**

[12](#)

Get in Touch

[14](#)

Hub Security At A Glance

Securely Hosted

The Hub is hosted on the **Google Cloud Platform** at UK data-centres, with nightly backups to AWS servers in the EU. Enjoy **unlimited data storage** and rapid implementation, with zero maintenance and no impact on your local IT.

Single Sign-On (SSO)

Setting up SSO is easy on your Hub, giving your users a secure, hassle-free way to login, and seamless access to your other third-party systems.

Two-Step Authentication

Google 2-Step Verification provides an extra layer of security logging in, and is compatible with leading authentication apps Duo Mobile and Google Authenticator.

ISO 27001 Certified

Pancentric is proud to be **ISO 27001:2013 certified** in Information Security Management, and The Hub is fully ISO compliant. Our impeccable security processes and robust infrastructure ensure your data is safe and secure.





Industry Recognised

Leading The Way

The Hub is proud to be recognised by the world's largest software marketplace, **G2**, as one of the industries top solutions for intranets and employee communications.

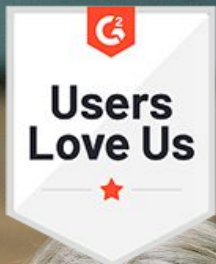
Our platform is a **High Performer** in the global marketplace for Employee Intranets, Employee Engagement and Internal Comms solutions, ranking **Top #4 in UK** and **Top #7 in Europe**, as well as **Top #8 worldwide for SME 'Mid-Market' organisations** (between 50 - 1,000 employees).



Users Love Us

G2 is a peer-review site, meaning our top rankings are generated by genuine user satisfaction ratings by real Hub customers. Thanks to [amazing feedback](#) by our happy customers, The Hub is proven to deliver you a solution that's easy to use, easy to manage, with outstanding customer support.





The Hub provides a robust, stable platform which has enabled us to centralise many strands of data that were previously held in multiple locations.

While on the one hand it can provide a virtual 'noticeboard', it also hosts a range of interactive forms which our staff can use to manage a multitude of activities.

We now use The Hub as a focal point for our internal communications.

Bailey Pittaway
Sales Support Assistant

Lycetts

Infrastructure Security

Google Cloud Hosted



All Hubs are securely hosted on the **Google Cloud Platform**, with data stored at UK-based data centres which adhere to the highest security levels.

For more information see:
<https://cloud.google.com/security/>

Nightly Backups



Backups of all Hubs are conducted nightly on **Amazon Web Services (AWS)** servers securely hosted in the EU (Dublin), and can be restored at short notice.

Bootstrap



The Hub utilises Bootstrap - the world's most popular open-source framework for building **fully responsive**, mobile-first platforms.

Bootstrap standardises The Hub's front-end, ensuring a fully responsive design that's well supported across all browsers and devices.

Environments



The Hub's development, staging and live environments are completely separate, with dedicated virtual servers and totally segregated networks.

Each Hub has a dedicated, logically separated database, providing isolation of client data from other users.

All user access requests pass through middleware to check validity and set specific Hub settings locking that request to a single logical environment.

Kubernetes



The Hub runs on Kubernetes, an open-source platform which allows for:

- 👉 **automated deployment;**
- 👉 **infinite scalability;**
- 👉 **effortless management.**

Employing Kubernetes ensures your Hub's environment grows with you and always maintains a high level of speed and performance.

Server Hardening



All servers are hardened in line with standard industry practices

Patching



Servers are **regularly patched** against known security vulnerabilities. Any patches are tested prior to use on staging environments, ensuring they do not adversely impact live environments.

Monitoring



24x7 monitoring and protection is performed by our dedicated in-house server management team.

Firewalls



Servers are secured behind 'default deny' firewall rules and are locked down to prevent any unauthorized access.

Software Security

Security Framework



All form and URL inputs are sanitised to protect the integrity of The Hub and to protect against:

- 👉 SQL injection (SQLi);
- 👉 Cross Site Scripting (XSS);
- 👉 Cross Site Request Forgery (CSRF)
- 👉 and other types of attack.

The Hub only runs over SSL and cannot be embedded into other systems.

Encryption



At rest

All client data is encrypted on both the Google Cloud Platform and AWS servers when at rest.

In transit

When in transit, all data between The Hub and your network is protected with encryption using HTTPS and TLS.

Penetration Tested



Pancentric conduct regular monitoring and testing of The Hub's environments via both internal and external penetration tests with our partners [NCC Group](#).

IP Restrictions



The Hub's 'IP Address' module can be configured to allow general access and use of single sign-on (SSO) to be locked down to a single or multiple IP addresses or ranges.

Anti-Virus



Uploaded files are immediately scanned for viruses, and any potentially compromising files are immediately deleted and our incident response team are alerted.

Audit Information



Audit logs of user activity are kept on all core database tables, and can be accessed (based on user permission level) in real-time via your Hub's Management Reports.

Product Security

Logging In



The Hub requires a primary user identifier (UID) to be entered alongside a password in order for users to log into the system. The UID can be set as either:

- ✚ **Email address;**
- ✚ **Mix of email & unique usernames.**

(NB: Users without an email associated with their account will receive all Hub comms via The Hub's internal InMail Box.)

Single Sign-On



Single sign-on (SSO) can be set-up as an alternative login method to entering a UID and password. SSO will automatically opt-in and authenticate users using your own existing systems and login information. Hub SSO integrations include:

- ✚ **Microsoft Azure Active Directory**
- ✚ **Office 365**
- ✚ **OKTA**
- ✚ **OneLogin**
- ✚ **Google**
- ✚ **Facebook**

Two Factor Authentication (2FA)



The Hub uses **Google 2-Step Verification** which can be manually turned on within your Hub Settings.

Google 2-Step Verification provides an extra layer of security when users login, by requiring an additional security passcode from an authentication app. The Hub is compatible with standard 2FA apps, including:

- ✚ **Google Authenticator**
- ✚ **Duo Mobile**

Permission-Based User Access



- ✚ Every module and feature has its own permission set governing access, editing and management rights. Create custom permission levels, 'User Types', and assign to specific users.
- ✚ Permissions are checked at run-time, making any changes instant without the need for logging out.
- ✚ Users cannot see modules or features they do not have permission to access.
- ✚ Hub Search will only return results based on the user's permissions.

Auto Logout



Each individual Hub Community can be configured to automatically log users out after a set period of inactivity:

- ✚ **After 5 minutes**
- ✚ **After 20 minutes**
- ✚ **After 40 minutes**
- ✚ **After 1 hour**

Content Moderation & Approval Processes



- ✚ Assign dedicated Viewers, Editors and Owners of specific content.
- ✚ Restrict viewing access or enable editing permissions on individual page-levels to specific users or groups.
- ✚ News has a workflow approval process. Editors must request content approval from an Approver or Owner to publish.

Custom Password Policy

Encryption



Passwords are encrypted using one-way hashes and a separate salt for each client. Common passwords are rejected.

Failed Logins



Accounts are temporarily locked out after five consecutive failed login attempts.

Password Resets



If a user resets their password, then any other logins with that user's credentials are immediately invalidated.

Password Policy



Your Hub's Settings have a configurable password policy, allowing you to set a Password Strength Template determining:

- 👉 **Minimum length;**
- 👉 **Character format.**

Logins Report



All login attempts are logged in the database.

Login history for individual users can be viewed in the User Activity Report.

Dedicated Hub Login Report consolidates all login attempts over a set period of time. The report has filterable parameters and details:

- 👉 **Total successful logins**
- 👉 **Total failed logins**
- 👉 **Total forgotten password requests**
- 👉 **Total of users who got their password wrong 5 times in a row**
- 👉 **Other Login Methods, including:**
 - Persistent cookies
 - Google Logins
 - Azure Logins
 - Other SSO Logins

Password Reuse



Configure Hub Settings to allow or prevent users from reusing old / previously used passwords when resetting their password.

Expiration



Set a password expiry period so that users must update their password after a specified number of days. (Default policy settings are that passwords never expire.)

Autocomplete



Set whether password autocomplete is allowed or disallowed.

Data Protection & Privacy

GDPR Compliant



Pancentric adheres to strict data protection rules, in line with our ISO certification.

The Hub is fully GDPR compliant, with dedicated data protection and privacy features enabling secure management, reporting and removal of user data.

Storing User Data



User data is stored in perpetuity by default, even after a user's profile is made 'Inactive'.

Hub Settings can be configured to allow for the automatic deletion / anonymising of inactive users after a set period of months, determined by you, to protect the data privacy of previous users.

Personal Data Report



Dedicated Subject Access Request (SAR) report displaying all data held on a specific user. The report shows:

- 👉 **Profile details;**
- 👉 **Personal contact information;**
- 👉 **All messages sent via Hub InMail;**
- 👉 **Comments left by user;**
- 👉 **Likes on content;**
- 👉 **Browsing history.**

Data Privacy Notice



A customisable Data Privacy Notice is displayed to users when they log into The Hub for the first time.

A mandatory checkbox accompanies the Data Privacy Notice, ensuring users must accept the policy in order to login.

Anonymising Users



- 👉 'Anonymising' user data permanently deletes a user's profile from The Hub's database, and scrambles all personal information associated with their profile.
- 👉 Anonymised user profiles are reduced to an '*Unknown User*' on all previous activity associated with their profile, i.e. past form submissions, comments, etc.
- 👉 Admin users with the correct permissions can manually 'Anonymise' user profiles, both individually and in bulk.

End-users can run a Personal Data Report on themselves only, to see the data held on them within The Hub.

Your Hub Admins can run a Personal Data Report on any user.

Company Processes & Policies

ISO Certified



Pancentric is ISO 27001 certified in Information Security Management, achieving zero non-conformities and demonstrating “exceptional monitoring, controls and support processes” to ensure all data is robust and secure.

The Hub is certified as a fully ISO 27001 compliant solution.

Controlled Access



Pancentric is a data processor.

Pancentric's access to client data is strictly controlled and only available to authorised personnel.

Security Policies



Pancentric has 33 ISO compliant security policies which are regularly reviewed and externally audited, including but limited to:

- ✦ Acceptable Use Policy
- ✦ Access Management Policy
- ✦ Antivirus & Malware Policy
- ✦ Acceptable Legislation
- ✦ Asset Management Policy
- ✦ Business Continuity Recovery Plan
- ✦ Change Management Policy
- ✦ Communications Policy
- ✦ Configuration Management Policy
- ✦ Corrective Action Procedure
- ✦ Cryptographic Control Policy
- ✦ Document Control Procedure
- ✦ Incident Management Policy
- ✦ Information Classification Policy
- ✦ Information Security Policy
- ✦ Internal Audit Policy
- ✦ IT Backup Policy
- ✦ Privacy & Personal Data Protection
- ✦ Risk Management Procedure
- ✦ Security Breach Incident Response Plan

Inhouse Development



All Hub development is carried out by our inhouse Development Team and maintained by our inhouse Operations Team.

Staff Security



Pancentric performs Enhanced DBS (Disclosure and Barring Services) background checks on all employees, covering complete criminal history, as well as a five year address and employment history and education verification.

Training



In collaboration with [Pen Test Partners](#), Pancentric conducts annual Information Security Awareness training for all staff, and runs secure coding workshops with our Hub developers.



The Hub is an excellent platform from which we can easily disseminate and host a wide range of content. What I like best is its many useful intuitive features and functionality – they clearly put a lot of thought into The Hub’s design.

The support from Pancentric (including set-up, deployment, development, and day-to-day support) is excellent and they are always open to new suggestions.

Alastair Moir
Head of Information & Research

TINDALL RILEY
TRUSTED SINCE 1855



Get In Touch

hub@pancentric.com | 020 7099 6370

hub.pancentric.com

The Hub c/o Pancentric Digital,
Level 30 The Leadenhall Building, 122 Leadenhall Street,
London, EC3V 4AB