imagen

# SECURITY FEATURES

**Protect your content and prevent unwanted access by securing your media within Imagen.**

**Secure data centres, Infosec policies and a range of advanced features combine to make sure your content is only available to trusted individuals or groups.**

## USER AUTHENTICATION

**Email/password and SSO (Single Sign On) authentication options for regulated user management.**

Imagen offers powerful options for identity management and authentication of users. Alongside basic Email and Password authenticated accounts, Imagen allows users to sign in using their existing corporate/enterprise credentials via secure SSO (Single Sign On).

## EXPIRING MEDIA LINKS

**Media URLs contain digitally signed access tokens with built in expiry time.**

Imagen digitally signs and dynamically updates links to media every 6 hours. This prevents unscrupulous users from uncovering and publishing the URL of the media object from the source code. Non-persistent URLs deter unauthorised sharing of links to your media files.

## GRANULAR PERMISSIONS

**Choose who can see your media and what they can do with it.**

Set up individual and group permissions with default access rights. Manage roles and responsibilities with granular permission sets, enable access to single media items or content sets at group or individual level. Ban or suspend users.

## SECURE DATA CENTRES

**Global network of Tier 4 datacentres deliver high performance and best in class security.**

Imagen uses the most secure public cloud infrastructure to safeguard your data in facilities that are protected by industry leading physical security systems and are compliant with a comprehensive portfolio of standards and regulations.

imagen

## WATERMARKING

**Overlay logos and text onto your media to deter piracy and prove ownership.**

Imagen can burn onscreen graphics into proxies before making them available for preview online or sharing via social media. Clean, high resolution copies can also be provided for trusted partners and customers but it is good practice to protect public facing content by overlaying a spoiler to deter copying and illegal distribution.

## SECURE DOWNLOADS

**Streaming and downloads use HTTPS – a secure method of exchanging data between the server and the client browser.**

All communication between the users' browser and Imagen is made over secure HTTP **with** HSTS connections **and modern TLS protocols**. That means requests for data or media files (either streamed or downloaded) are encrypted – making it much tougher for anyone to intercept or steal content or information.

## SUNRISE & SUNSET DATES

**Choose a date range for content to be available for individuals or groups.**

Sometimes you need to make time sensitive content available to an individual or a group for a specific length of time and no longer – during a licensing agreement, or when distributing previews ahead of release date. Imagen gives you the power to set dates and times to control access to your media.

## GEO-IP BLOCKING

**Choose which regions are able to access your media by IP address range.**

For licensing or security reasons you may wish to block internet traffic from geographical locations based on an IP address. Preventing specific territories from accessing your media via your Imagen platform is easily achieved using Imagen's GEO-IP filters.

imagen

# IMAGEN INFO-SECURITY, RISK & COMPLIANCE PROGRAM

**Security plays an important part in every area of our business - from software development coding practices through to system development and infrastructure. Our customers rely on us not just for the development of stable video management software but also to ensure that their media, metadata, personal and financial information remains secure.**

## SECURITY IN DEVELOPMENT

Security at Imagen starts with good project management supported by industry recognised practices & procedures - as documented in our **SECURE DEVELOPMENT POLICY.** To ensure demands and solutions evolve through a collaborative effort our self-organising and cross functional teams have adopted the industry recognised **AGILE** methodology for project management.

Imagen have adopted the following **OWASP** principles, which include:

- minimising the attack surface area
- establishing secure defaults
- following least privilege principles
- adopting defence in depth principles
- always fail securely
- don't trust services by default
- separation of duties
- avoiding security by obscurity
- keeping security simple
- fixing security issues correctly

## VULNERABILITY & PENETRATION TESTING

Our software coding is **PENETRATION TESTED** annually by industry recognised **CHECK/CREST** approved third parties. This program is further supported monthly by scans of all system assets conducted by **NESSUS VULNERABILITY SCANS TO PCI-DSS STANDARDS.**

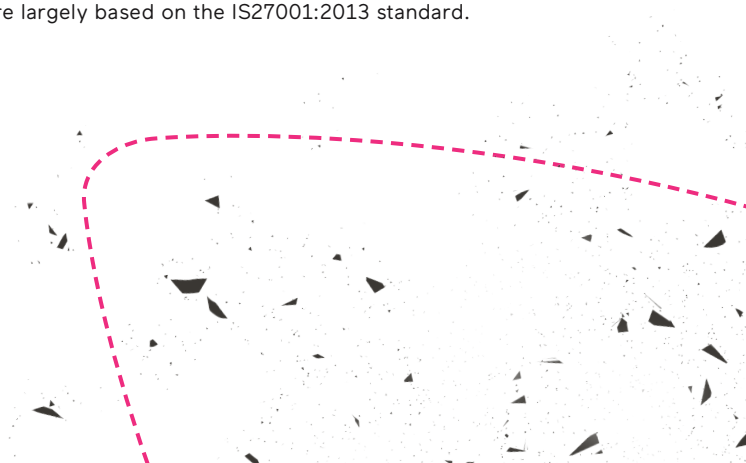
## ACCESS CONTROLS

Access to development code, IT assets and systems, buildings and in particular customer services **are** strictly controlled by our documented **ACCESS CONTROL POLICY**. Access is granted to approved users and audits conducted of records retained for starters, leavers and job role changes. Access control and configuration data is retained in encrypted vaulted systems which are logged and monitored.

## ACCREDITED CERTIFICATION AND AUDITS STANDARDS

Imagen seek to provide assurances to customers in relation to our processes, for both the quality of the processes we adopt and information security. For that reason, we have adopted an **INTERNAL AUDIT PROCESS** which is conducted by our own on internal Information Security, Risk and Compliance Team. This is further supported by certification to **ACCREDITED ISO9001 & ISO27001 STANDARDS BY AN EXTERNAL BODY RECOGNISED BY THE INTERNATIONAL ACCREDITATION FORUM**.

In addition to the above, Imagen are **ALSO CYBER SECURITY ESSENTIALS** certified **and also have accredited security certification** with the **DIGITAL PRODUCTION PARTNERSHIP**. This is an initiative formed jointly by the UK's public service broadcasters to help producers and broadcasters maximise benefits of digital television production - the controls of which are largely based on the IS27001:2013 standard.



imagen

## SUPPLIER POLICY

For continued assurances in regard to protecting assets and continuity of service, Imagen's documented **SUPPLIER POLICY** requires our selection of vendors to be vetted.

Suppliers engaged in delivery of customer services shall be vetted for financial stability, maintain or provide documented instructions for the processing of personal data compliant with GDPR article 28, maintains CSA STAR certification, ISO27001:2013, ISO27017:2015, ISO270018:2014. ISO2000-1:2011 and ISO9001:2015 accredited certifications. News feeds, special interest groups, industry communications channels and the general press are all monitored by the Info-Security, Risk and Compliance Team for security, financial or other irregularities which may impact on service delivery objectives.

## BUSINESS CONTINUITY

To meet with Imagen's documented **BUSINESS CONTINUITY POLICY,** selection of key suppliers must consider adoption of and certification to **ISO22301:212** accredited standard. The adoption of suppliers providing such assurances is accepted by Imagen, as meeting with our own policy requirements.

To support the Business Continuity Policy, Imagen adopts a rigorous policy for the **DATA BACKUP PROGRAM** and retention of customer metadata and user data by default. **M**any additional configurable options for greater levels of data retention and recovery **can** secure the entire media estate, if required. These processes are also included in the Info-Security, Risk and Compliance audit programs.

## GDPR & PCI-DSS

Imagen are aware of our obligations under **DATA PRIVACY LAWS** (both globally and under GDPR, DPA2018. PECA). We also aware of the impact of these regulations on our customers, as such, reviews are conducted regularly to ensure Imagen is compliant with its own data privacy obligations and functionality of our services delivery platforms provides customers with the controls to meet with their own data privacy obligations.

Part of the functionality of our service platforms includes options to process **CREDIT CARD PAYMENTS**. Imagen are aware of our obligations under the **PAYMENT CARD INDUSTRY - DATA SECURITY STANDARDS. A**s such we work with each client to ascertain the level or processing required **to** ensure compliance. Clients adopting standard delivery payment mechanisms, via the services platform can rest assured of conformance with these requirements by design and default.


**WE ARE IMAGEN.**

Drive engagement, generate revenue and transform your business with the world's smartest video management platform.

**LONDON**

16 Kirby St, Second Floor
London, EC1N 8TS

hello@imagen.io
+44 (0)1954 262000

**CAMBRIDGE**

1 Grange Court, Covent Garden,
Willingham, CB24 5AH

hello@imagen.io
+44 (0)1954 262000

**NEW YORK**

106 West 32nd Street, 2nd Floor
Office #135, New York, NY

helloUS@imagen.io
+1 (857) 574 9847