Data and Encryption Policies

Certifications and Assessments

IR35 Shield (“we”, “us” or “our”) is PCI-DSS certified and complies with GDPR regulations.

Data Centers and Location

IR35 Shield production services are hosted on Amazon Web Services’ (“AWS”) EC2 platform. The physical servers are located in AWS’s EC2 data centres. As of this date, AWS has certifications for compliance with ISO/IEC 27001:2013, 27017:2015 and 27018:2014, is certified as a PCI DSS 3.2 Level 1 Service Provider, and undergoes SOC 1, SOC 2 and SOC 3 audits (with semi-annual reports). Additional details about AWS’ compliance programs, can be found at AWS’ website.
All user content is stored within the United Kingdom. IR35 Shield’s production environment is hosted on an AWS EC2 platform. User data is stored in AWS EC2, S3, RDS and ElastiCache. User content can also be found in IR35 Shield backups, which are stored in AWS EC2 and S3.
We currently do not offer customers the option of hosting IR35 Shield on a private server, or to otherwise use IR35 Shield on a separate infrastructure.

Production Environment

We maintain separate and distinct production, staging, and development environments for IR35 Shield.
To access IR35 Shield’s production environment and authorised members of IR35 Shield's software engineering team (“Authorised Personnel”) authenticate to our Amazon VPC using strong passwords and 2FA. For Authorised Personnel, any workstations running Windows or macOS must be running current and active anti-virus software. Those members are also trained not to replicate non-public user data stored in IR35 Shield’s production environment onto their workstations or mobile devices.

Network Security

IR35 Shield uses an automated monitoring system to detect and alert against DDoS attacks. AWS Network ACL and Security Groups are used to restrict access to IR35 Shield's systems as appropriate to their role. Public access is restricted to port 443 and 80 on the network load balancers for public traffic.

Login security

Logging in to IR35 Shield requires an email and a password. IR35 Shield enforces a minimum password of 8 characters, with at least one upper case character and one numerical character. IR35 Shield also displays a "password strength" indicator, to help users choose an appropriately secure password. Repeated failed login attempts trigger a 60 second lock before a user can retry. Passwords are stored in a hashed form. Upon account creation and password reset IR35 Shield will check the email submitted by the user and, in the case of a match, send a link to the associated email that will enable the user to create a new password. Password complexity and session length requirements cannot be customised within the app. Multi Factor Authentication (MFA), based on the Internet Engineering Task Force standard RFC 6238, can be enabled by each individual user for their own account or, in the case of Shield for Business or Shield Manager customers, organisation-wide. MFA is automatically enforced for privileged users (Admin).

Vulnerability Detection and Penetration Testing

IR35 Shield has made a commitment to ongoing security by commissioning a full Penetration Test on an annual basis. Our most recent Penetration Test was completed in July 2020, with the results showing no outstanding vulnerability rated higher than "Medium". Our development team has assessed the risk impact of each remaining vulnerability, and are comfortable that either they; i) do not require remediation or ii) the specific threat level is low to our business and therefore remediation will be scheduled when resource is available.

Access Control

All user data stored in IR35 Shield is protected in accordance with our obligations in the IR35 Shield Privacy Policy, and access to such data by Authorised Personnel is based on the principle of least privilege. Only Authorised Personnel have direct access to IR35 Shield's production systems. Those who do have direct access to production systems are only permitted to view user data stored in IR35 Shield in the aggregate, for troubleshooting purposes or as otherwise permitted in IR35 Shield's Privacy Policy.

IR35 Shield maintains a list of Authorised Personnel with access to the production environment. On hiring, these members undergo background checks and are approved by IR35 Shield's Management Team. IR35 Shield also maintains a list of personnel who are permitted to access IR35 Shield code, as well as the development and staging environments.

Trained members of the IR35 Shield customer support team also have case-specific, limited access to user data stored in IR35 Shield through restricted access customer support tools. By submitting a support ticket or email, an IR35 Shield user gives permission to authorised members of the support and / or development team to view data pertaining to the ticket, as per the IR35 Shield Terms of Service agreement. Without an active ticket, data is not authorised to be accessed by any members of the IR35 Shield support team.

Upon role change or leaving the company, the production credentials of Authorised Personnel are deactivated, and their sessions are forcibly logged out. Thereafter, all such accounts are removed or changed.

Third Party Access

User data may be shared by IR35 Shield with third-party service providers (a user's email address for an email delivery provider, for example) pursuant to IR35 Shield's Privacy Policy and in compliance with IR35 Shield's applicable signed service agreements.

Physical Security

Our offices share buildings with other companies. Visitors must wait in our secured reception area until allowed entry by an authorised person. Employee access to physical facilities is protected by electronic badge readers and building security. CCTV covers entry and exit points 24/7 with logs made available to us internally upon request.
IR35 Shield's production services are hosted on Amazon Web Services' ("AWS") platform. The physical servers are located in AWS' secure data centers.1 We require that production critical data is never to be stored by those with privileged access on physical media outside of our data hosting provider's production environments. See link above for information on AWS' compliance programs.

Encryption In-Transit

IR35 Shield uses industry standard Transport Layer Security ("TLS") to create a secure connection using at least 128-bit Advanced Encryption Standard ("AES") encryption. This includes all data sent between user devices and the IR35 Shield servers. There is no non-TLS option for connecting to IR35 Shield. All connections are made securely over HTTPS. Any requests made by HTTP are automatically redirected to HTTPS.

Encryption at rest

All our data is stored using full disk, industry-standard AES encryption. File uploads are stored in Amazon's S3 service. Each such upload is not publicly accessible through S3 directly. They are only accessible by internal IR35 Shield systems and IR35 Shield's AWS dashboard. File uploads are encrypted using Amazon S3 server side 256-bit AES encryption. The encryption, key management, and decryption process is inspected and verified internally by Amazon on a regular basis as part of their existing audit process. All IR35 Shield backups are encrypted with AES encryption.

Encryption Keys

Encryption keys for IR35 Shield uploads, stored in S3, are managed by Amazon. The encryption, key management, and decryption process is inspected and verified internally by Amazon on a regular basis as part of their existing audit process. Encryption keys for IR35 Shield uploads managed by our team are rotated upon relevant changes of roles or employment status. Encryption keys managed by our team are not stored outside of IR35 Shield's production backup environment and are managed by our development team. IR35 Shield backups are of the entire data set, so they are encrypted using a shared key.

Data Deletion, Retention and Processing

IR35 Shield's core business relies on intelligence gained from data collected when users complete online assessments. Please view our Privacy Policy for a full detailed description of how data will be processed and retained, and on what basis.

User Team Management and Access

Users for an IR35 Shield for Business account will be set via an authorised member of IR35 Shield's support team. It is not possible to limit the geolocations allowed to access data within IR35 Shield. Data can be accessed by users who have access to such data within the app from any geolocation. All third-party developer access to user data stored in IR35 Shield is via the API which includes strict authorization checks. All Authorised Personnel go through strict security group/firewall rules which limits access to authorised instance roles on authorised ports required for them to fulfill their role.

Development, Patch and Configuration Management

All changes to the IR35 Shield production system, be they code or system configuration changes, require review prior to deployment to the production environment. Thousands of automated unit tests are run against all production code prior to deployment. All changes to IR35 Shield's code are tested in a staging environment prior to deployment to production. Patches to the IR35 Shield web client are deployed on a rolling basis. IR35 Shield production servers are managed via a centralised configuration system. All IR35 Shield system changes are internally acceptance tested depending on their level of security and stability impact, with critical patches deployable well within 24 hours of availability as appropriate.
We restrict access as noted above and maintain separate lists of relevant roles with access to source code, development, staging, and production environments. We use source code management tools and repositories. All production servers are running a LTS (Long Term Support) distribution of their operating system to ensure timely updates are available. CVE lists and notifications are actively monitored and any systems can be patched in a timeline relevant to the severity of the issue. A centralised configuration system is used for the management of production servers, and when needed a patch can be deployed within hours of its availability.

Event Logging

All IR35 Shield API calls and application logs are kept for our internal purposes without sensitive information (no full user tokens, no user generated content), and are available only for authorised employees as required by their role for monitoring of IR35 Shield to ensure service availability and performance and to prevent abuse.

Backup, Business Continuity, and Disaster Recovery Policy

Backup Policy

Data entered into IR35 Shield is backed up regularly. All backups are encrypted and stored at multiple offsite locations to help ensure that they are available in the unlikely event that a restore is necessary.
Files uploaded to IR35 Shield are not backed up on the same schedule, and instead rely on Amazon S3's internal redundancy mechanism. Any encrypted backups can only be decrypted by members of the IR35 Shield operations team who have received training and have been authorised to decrypt the backups.
Because user data stored in IR35 Shield is on a shared infrastructure, it is not possible for us to recover a subset of that information from backups.

Backup Interval

A full backup snapshot of the primary database is taken once every 24 hours and, alongside this, we keep a 5 minute incremental backup of database transactions.

Backup Storage

All IR35 Shield backups are retained in AWS RDS for 14 days.
Only authorised members of the IR35 Shield operations team have access to the backup locations, so that they are able to monitor the performance of the backup processes, and in the very unlikely event that a restore becomes necessary.
Attachments directly uploaded to IR35 Shield are handled differently than the primary database backups. To backup file attachments, IR35 Shield primarily relies on S3's internal redundancy mechanism, which Amazon states provides 99.99% yearly data durability.

Business Continuity

The IR35 Shield development team has designed systems to keep the service running even if the underlying infrastructure experiences an outage or another significant issue. If service of the AWS Availability Zone that hosts IR35 Shield was interrupted, we have systems in place to failover to another Availability Zone in order to restore service within one hour during business hours, and twenty four hours outside of business hours.

Disaster Recovery

In the unlikely event that an Amazon availability zone has long-term service interruptions, IR35 Shield has been designed to recover with limited service interruption and a target maximum of 5 minutes of data loss.
In the even more unlikely event that IR35 Shield's entire AWS region is irrecoverably lost, we will restore servers with the assistance of automated configuration systems. In this event, IR35 Shield's systems are designed to recover user data as quickly as reasonably possible, with a target of no more than 24 hours of data loss.
IR35 Shield's development team regularly tests the various components of its Business Continuity architecture to ensure continued operations.
IR35 Shield does not currently run anything like Chaos Monkey.

Critical Incidents and Response

IR35 Shield does not have an SLA or credit policy.
Any support tickets received through IR35 Shield software or relating to IR35 Shield services will be assessed according to their impact on *system-wide* service within one business hour. We have three categories of system-wide impact - no impact, important and critical. Once a ticket has been deemed to have no system-wide impact, it will be prioritised, categorised and reported to the development team according to IR35 Shield support team best practice.
Table 1: System-wide Impact Levels:

Level	Description	Resolution	Examples
Critical	IR35 Shield is not available or is unusable for all customers	Work begins within 1 business hour from fault report, temporary resolution within 4 hours, final resolution within 8 hours.	The site is not responding; all text on the site is being translated into elven runes.
Important	Service or performance is substantially degraded for all customers in a way that prevents normal use	Work begins within 2 business hours from fault report, temporary resolution within 48 hours, final resolution within 5 days.	Users can log in, but cannot access a report. Users can log in, but invitations will not send.
No System-wide Impact	IR35 Shield is running for all customers - any reports of critical system impact are localised to one account	Work is scheduled and customer is informed according to IR35 Shield support team best practice	Report has displayed incorrect information for a contractor, page load is taking a longer time than usual

Employee Policies

Anti-Virus

For Authorised Personnel, any workstations running Windows or macOS used for access to the production environment must be running update-to-date and active antivirus software with real-time monitoring and at-least-daily updates.
Authorised Personnel may choose to run Linux as their workstation operating system. Given the inadequate state of Linux antivirus software and the lack of prevalence of viruses for that platform, our policy does not require those workstations to run antivirus. All of the existing controls for Authorised Personnel, including restricting access from those workstations to the production environment and with no replication of user data onto those workstations, still apply.

Security Awareness and Confidentiality

Security awareness and user data access policies are covered during our employee onboarding as appropriate to the role and employees are updated as relevant policies or practices change. Our employees also sign a confidentiality agreement.
In the event that a security policy is breached by an employee, IR35 Shield reserves the right to determine the appropriate response, which may include termination.

Background Checks

All our employees undergo an interview process before hiring. Our employees with direct access to the production environment undergo a background check. Other employees may undergo a check depending on their role (e.g., academic for legal roles or credit for finance roles). Appropriate NDAs are in place with third parties as required.

Maintenance Policy

Planned Maintenance

When it is necessary to perform planned maintenance on IR35 Shield services, IR35 Shield will perform the work during off-peak system times or overnight. We will make reasonable efforts to announce maintenance procedures that could potentially impact users of IR35 Shield at least 24 hours prior to the event.

Potential Maintenance Windows

Our services are based around UK employment law and, as such, we use UK timezones to decide our Service Maintenance Windows (9pm to 12am UK time GMT or BST depending on date). These windows have been selected with the goal of minimizing service downtime, slowness, or other impact to the people and businesses that rely on IR35 Shield.
We do our best to make outages as short as possible. Additionally, our maintenance schedule will frequently be evaluated to ensure that we keep user impact as low as reasonably possible. Should we need to reschedule these windows, the updated schedule will be announced on our Status Blog and Twitter accounts with reasonable advance notice.

Unplanned Maintenance

Due to unforeseen events, we may have to infrequently perform unplanned maintenance on IR35 Shield infrastructure or software components. This maintenance might cause some or all of the IR35 Shield services to be inaccessible by our users for a period of time. It is our goal to do this as infrequently as possible. Any unplanned or emergency maintenance that causes IR35 Shield to be inaccessible will be announced with as much advance notice as reasonably possible. As with planned maintenance, we do our best to minimise disruption caused by service outages.

Links

1 https://aws.amazon.com/security/

Changelog

- **October 2020 (v1.5)** - updated EU to United Kingdom after migration from Dublin to London. Encryption At-Rest policy reinstated and now live. Multi Factor Authentication (MFA) added.
- **August 2020 (v1.4)** - addition of upgraded password requirements, and penetration testing schedule and results. Removal of scheduled Encryption At-Rest policy and scheduled Business Continuity policy
- **December 2019 (v1.3)** - links updated
- **November 2019 (v1.2)** - issued with data retention / deletion now pointing to new Privacy Policy, new timeframe for Encryption at Rest, and Backup Storage policy adapted to reflect current procedure
- **October 2019 (v1.1)** - issued with new timeframe on Business Continuity and Encryption at Rest
- **July 2019 (v1.0)** - goes live