Actus
Performance Management Software

Actus Software Data Security Policy

Advance Change Ltd is an ISO 27001 accredited provider of SaaS Actus™ Performance Management Software and data security is of the utmost importance to us. We only host our data with fully accredited and respected UK organisations and all data is retained solely within the UK.

General Data Security Principles

There are a number of ways in which we ensure that your data is securely held, using our 3rd party provider Memset Ltd, and these include:

Physical and Environmental Server Security

- ISO 27001 certified data centres
- Comprehensive CCTV coverage with footage retained for 90 days
- Biometric and/or RFID badge controlled access to data halls
- Physical access limited to specific necessary personnel
- Stand-off fenced perimeters in place
- At least N+1 UPS, generators and HVAC
- FM-200 fire suppression
- Continuous Building Management System monitoring

HR Security

- All Actus staff and those of our third party data processor are CRB and background checked
- Only our Systems Administrators have access to customer servers
- Access to customer servers is gained via personal keys, and all access is logged
- Logs and activity are routinely checked by our Head of Security
- Organisational separation of those who have physical access to servers, and those who know what is on the servers
- Mandatory confidentiality agreements and security awareness (including data protection) training for all staff

Datacentre compliance

1. ISO 27001:2013 certified hosting services and data centres
2. ISO 9001 and 14001 certified
3. PGA accredited to provide Official (IL2-IL3) services
4. Accredited to provide Official classified services via encrypted PSN overlay

Hacking prevention

- Managed Platform SLA, Packet Patrol™ managed firewall
- Perimeter Patrol™ vulnerability scanning
- Penetration Patrol™ intrusion detection

Infrastructure Security

In order to ensure the security of the Actus application and all server information we employ a combination of current, recommended solutions.

1. **Intrusion Prevention System (IPS) & Intrusion Detection System (IDS) - SNORT**

   We use SNORT with shared community object rulesets and monitor via automatically triggered alerts. This takes the form of instant e-mail notification for Priority 1 alerts. All SNORT alerts are transferred into our BASE interface where we can find an exact time and signatures that were detected.

2. **Additional Security- Web Application Firewall (WAF)**

   Additional firewalls are provided by our Service Provider. Therefore, the only service that is widely accessible is https, all others like ssh and sftp are firewalled:

   - **Port 443**
     We have forced all users to use SSL (https), so none of our services can be reached via non-encrypted connection. The only resource viewable by clients is our Actus Software interface

   - **Port 8080**
     There are other resources running on port 8080 but they are restricted at the server firewall. Database access, that runs on https, is IP Address whitelisted by apache itself and is only accessible for developers and main office via a monitored list of the IP addresses

User Security

1. **Password Security –** Passwords are required to be 8 - 40 characters long; contain one lower case letter, one uppercase letter, one number and one symbol
2. **Optional enforced password change –** Period can be set at company level
3. **Optional 2-factor authentication** – This can be enabled at company or user profile level accessible via email or mobile device
4. **IP Whitelisted downloads** – Downloading of documents can be restricted to certain whitelisted IP addresses at company level
5. **IP Whitelisted access** – System access can be restricted to certain whitelisted IP addresses at company or user profile level

Transfer of Data

Actus will only transfer data via secure encrypted solutions which have been agreed with the client. Encrypted solutions shall be compliant with all relevant agreements, laws, and regulations. Secure management processes are monitored regularly as part of our ISO accreditation and back up and test data are subject to the same security protocols.

Hosting, back up and disposal of data

Servers

1. Main server: 8 core CPUs and high-capacity SSD disks are in a RAID (6) configuration, which means that any two disks can fail at the same time without data loss

2. Offsite backup servers which are proactively monitored and any failed disks can be replaced immediately.

Frequency of Back Up

The live application database is backed up hourly from the main server to the offsite backup server (also held in the UK) and aims to provide minimum risk of data loss.

Additionally, an overnight data extract is updated to a 3rd UK server location to ensure that risk of data loss is further reduced.

1. In the event of a catastrophic server loss, in our initial 2 sites, or other disaster, a maximum of 1 days' data is at risk
2. In the event of a single disk failure, the database should be recoverable to the last committed transaction
3. In the event of a database corruption, the database would be recoverable to the most recent 'clean' backup. This is a maximum of 60 minutes prior

Maximum Recovery Times

1. Automated daily backups are kept for 10 days so any instances of data corruption, system's failure or data input errors can be recovered
2. In the event of a failure requiring database recovery IT infrastructure, the recovery activity is assigned critical priority
3. In the event of a catastrophic machine loss or other major disaster, the policy expectation is that priority data will be recovered within three working days

Disposal of Data by Actus

On termination of the Agreement for any reason:

1. access to the Actus Software shall cease and all licenses granted under the Agreement shall immediately terminate
2. each party shall return and make no further use of any equipment, property, documentation and other items (and all copies of them) belonging to the other party
3. the Customer is responsible for downloading any personal data that they wish to retain using existing Actus Software functionality
4. Actus will destroy or otherwise dispose of any of the Customer Data in its possession 60 days after termination, unless a data extract is requested 14 days ahead of the termination date. In this event Actus shall use reasonable commercial endeavors to provide the data to the Customer in a CSV file within 60 days of the termination date on condition that the Customer has paid all outstanding fees and charges due to Actus. Actus reserves the right to charge up to £500 per 500 Users, for the administration and provision of said CSV file

5. the accrued rights, remedies, obligations or liabilities of the parties as at termination, or the continuation after termination of any provision expressly stated to survive or implicitly surviving termination, shall not be affected or prejudiced

6. Hard disks are physically destroyed or securely erased and disposed of by an authorised WEEE disposal company. Records of all such disposals are maintained in order to provide evidence of these activities within a Media Destruction Log

7. Other forms of media, e.g. smartphone SIMs (although these are not used to transfer client data), are similarly securely erased or destroyed and records kept within the Media Destruction Log

Disposal of Data by our Third Party Processor Memset

Memset maintains a stringent policy on the forensically effective logical and physical destruction of Customer Hosted Data on termination of individual data hosting resources. Full details of this are available via this link: https://www.memset.com/about-us/data-destruction-practises/.

GDPR - Right to Audit

Actus is responsible for auditing its third-party data processors for GDPR compliance. We will also support our Customers in their own GDPR audit responsibilities as long as we are given reasonable warning, and these do not interfere with day to day business processes or pose a risk to data security.

System Availability

Actus Software is responsible for managing their third-party hosting providers to maintain an expected system uptime of 99.95%, excluding maintenance.

In the rare event of unscheduled maintenance due to urgent issue resolution, Actus Software will inform the Client at the earliest opportunity of the issue, likely downtime and inform them as soon as it is resolved.

As this is software provided over the web, Actus Software cannot warrant that the Customer's use of the Services will be completely uninterrupted or error-free. They cannot be held responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Customer acknowledges that the Services and Documentation may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

Data breaches

In the unlikely event of a data breach, Actus will immediately investigate the cause in order to address and rectify the breach. This will be logged with the ICO, in line with GDPR requirements, and notify the customer with the extent of the breach, the mitigation and next steps within 48 hours.

Client responsibilities

Our clients are responsible for ensuring that sensible access controls are enforced by users such as keeping passwords secure and logging out of shared devices. It is also the client's responsibility to ensure that any nominated HR Admin users who have increased internal access to data are appropriately selected and monitored.

Privacy

Advance Change Ltd maintains a strong privacy policy to protect customer data, we will be following the guidance provided by the ICO on GDPR as it is released. We also work closely with an external, specialist data protection advisor. Advance Change Ltd does not own customer data or share it with third parties without prior written consent. Advance Change Ltd also allows customers to take their data with them, should they decide to stop using Advance Change Ltd.'s services. The full privacy policy is available on our website.

G-Cloud Registration

The security of your data is of the utmost importance to us, and UK public sector will be pleased to note that we are registered on the Digital Marketplace, also known as G-cloud, which means we have been accredited as secure enough to provide cloud services to government.

Security FAQ

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 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 Advance Change Ltd.

Are you registered with the ICO?

We are registered with the ICO with the number: ZA000335

Does Actus Software offer SSL connectivity?

All access to the application data is via the 256-bit SSL encryption, additional optional security measures can also be enforced such as specific IP access only and 2 step authentication.

Does Advance Change Ltd transfer data under the EU-U.S. Privacy Shield scheme?

The EU-U.S. Privacy Shield framework replaced the Safe Harbor framework in August 2016. It was approved by the European Commission pending a review in September 2017 and is currently under review. The Privacy Shield continues to require the U.S. to monitor, uphold and enforce protections for the rights and freedoms of individuals in the EU to EU standards under the GDPR when their personal data is transferred to organisations in the U.S.

The Department of Commerce in the U.S. oversees certification under the Privacy Shield scheme, however such certification is still voluntary and self-managed by individual organisations. The list of scheme participants can be viewed at https://www.privacyshield.gov/list.

Actus Software hosts and processes all client data in the UK; although as a business we use Google as our email provider and Sharpspring as our CRM both of which are American based firms which means that email addresses and names may be processed in one of these two systems.

How will you secure your EU client's data after Brexit?

Advance Change Ltd continues to follow the high standards set by the GDPR and following the UK's departure from the European Union in March 2019 will continue to ensure adherence to the same level of compliance. We will achieve this through the continued use of Standard Contractual (EU Model) Clauses in all our service agreements involving the processing of EU-based personal data.

Who owns the data that my organisation stores on Actus Software?

All of the data on Actus Software belongs to the customer, and it can be extracted upon request, should it be necessary.

Is my data subject to the Patriot Act?

The Patriot Act, passed in 2001 by the US states, 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. Advance Change Ltd is a UK company and uses UK-based hosting providers for our European customers. We follow the high standards set by the GDPR and utilise Standard Contractual (EU Model) Clauses in all our service agreements involving EU-based personal data.