GRAPHICAL DATA

Security of Apps and Business (Self Hosted)

Service Overview

The application is hosted by the customer internally on their own infrastructure and is accessed over their intranet.

GD will act in a support role to the application, should any issues arise (including code and software stack, but not including hardware or data content). To fulfill this role, Graphical require adequate remote access to perform diagnostics on the application.

Security Organisation and Policy

QU. Do you do personnel screening for employees and contractors.

Graphical Data operate a standard screening process when hiring any employees or contractors. The standards we require from each prospective employee are:

- application, CV details, background (experience, qualifications)
- interviews to verify suitability.
- professional references from at least 2 employers
- identity must be verified by appropriate means (license/passport)
- criminal record background check on all potential employees and
- contractors or Basic Criminal Disclosure.

QU. Do you have a security awareness program with employees and contractors?

Graphical Data operate monthly reviews attended by all employees to discuss any recent incidents, concerns and/or policy queries. Policy documentation is available to all employees via the GD intranet. Graphical Data has not suffered information security related incidents since we started business

QU. Do you have defined and documented escalation procedure for fault management and major incident / security incident handling?

All incidents or problems are received, dealt with and recorded by our Service Desk system.
The incident or problem is identified and classified into the appropriate severity level (Low, Medium, High and Critical) using the information gathered from the notification.
When the nature of the issue and its severity level have been determined, the resolution process begins - it is sent to the appropriate owner. If possible, the issue will be corrected quickly. However, if the nature of the problem means it may take some time to properly investigate, the first objective is to find a workaround solution.
If an issue is identified as being a major incident, extra resource will be brought in to deal appropriately, including Service Manager and/or Technical Director.
All issues are recorded and kept on our internal system, enabling auditing and reporting.

QU. Do you have a documented security policy and/or standard to deliver security requirements appropriate for the service and its operation.

Graphical Data have internal guidelines which include statements on the following:

- Information Security, including Data Storage, Processing and Transmission guidelines.

- Resiliency Plans, including Data, Applications and Operations (hardware and software).
- Security Information - physical and infrastructure security, employee training etc.
- Software Development - procedures that should be followed to ensure secure and stable software, testing and validation methods to be used, identify who is responsible for managing and maintaining these
- Auditing and Performance Measuring - protecting, securing and auditing access to sensitive resources, measuring response times and rate of defining and addressing issues, fault management.

While Not based on any definite standard, GD are familiar with the principles of ISO27001, as well as ITIL Best Practices.

GD is currently certified with ISO27001, Certification achieved in December 2018.

QU. Do your employees (permanent, temporary and contract) sign a document indicating they have read and understood your organisations security and privacy policies?

All employees are required to complete a security policy induction, which is regularly followed up during our monthly reviews. Whilst there is no official document relating specifically to this, all employees are required to sign a confidentiality agreement.

Customer Data Security

Qu. Who; in terms company or subcontractors, will be involved in processing the data provided by the customer

A list of Graphical Data employees who will be able to access information supplied and owned by the client can be provided upon request.

For up to date information, please contact info@graphicaldata.co.uk

Qu. Where external or third-party companies are used, please provide connection & network topology diagrams

No such arrangements exist.

Qu. Please provide detail of where (geographic locations and physical/logical technical equipment) and how Client data will be processed.

Graphical Data do not process any Client data - it is all held behind their own firewalls. The service will only require Graphical Data to perform remote diagnostics on the App using a secure VPN tunnel to the specific Server/VM. This will be achieved using a dedicated Graphical Data terminal which will be fully secured and maintained in a physically secure environment on Graphical Data premises.

Qu. Please provide detail of where (geographic locations and physical/logical technical equipment) and how Client data will be stored (e.g. multiplex, server, platform, disk or array configuration).

Graphical Data will not store any client data.

Qu. Please give full details of data backup procedures, including type (full, differential etc), media, schedules, locations, off-site, recovery tests etc.

Full backups of data and relevant systems are made daily and at least 30 generations at any one time are stored. Code is versioned with a full history going back to its beginning is stored in at least 3 secure locations, two of which are off-site to GD office.

All backups are labeled, encrypted and stored appropriately identifiable as to where and when they came from. Monthly tests are carried out to test the recovery procedure.

Qu. Where client customer data is stored, is it encrypted at all times? Please provide details in either case.

Graphical Data will not store any client data.

Qu. Please provide details of any cryptographic techniques in use including any methods of managing cryptographic keys?

As standard, Graphical Data uses AES full disc encryption with strong passwords and keyfiles to store their internal code and data.

Any cryptographic keys or certificates used are managed in an internal PKI.

Qu. How is ALL access to client data controlled, tracked and audited?

Access would be through a dedicated machine which would have limited user access except to specified personnel and all access would be logged. Automated logs are generated and maintained in a secure environment to enable audit trails for review.

Qu. How does the data storage system defend/monitor against brute force attacks?

Passwords and keyfiles used for encryption are separate for each location. They are randomly selected with a minimum length of 16 characters. Passwords and keyfiles are changed annually. Close care is taken for the secure containers not to leave their owners and each employee is trained not to share any security data with third parties, this also includes policies and procedures used.

Any customer information that Graphical Data receive is treated as Confidential and of High Importance, as well as being subject to an existing NDA agreement.

Qu. What are your documented data handling, storage & disposal processes?

Paper- Paper documents containing restricted data must be stored in a secured location such as locked office furniture, locked offices, and other locations specifically dedicated to secure storage of records when not in use. Crosscut shred or pulp all highly sensitive information in paper form including all transitory work products (e.g., unused copies, drafts, notes) to ensure physical destruction beyond ability to recover.

Removable Media- Restricted data stored on CD, DVD, BRD, or disk, must be encrypted. The media must be stored in a secured location when not in use or properly destroyed. Removable media must be destroyed by complete physical destruction of the media beyond ability to recover.

Flash Drives - Restricted data stored on a flash drive must be password protected and the data encrypted. The flash drive must be stored in a secured area when not in use or data properly destroyed. If the flash drive is going to be repurposed or destroyed, then the electronic storage device must be wiped with a multiple pass secure overwrite prior to being repurposed.

Electronic Documents - Anyone with access to electronic documents that contain restricted data must comply with the following requirements:

1. Enable password protection using a strong complex password.
2. Enabled full disk encryption to protect from data theft.

Physical and Environmental Security

Qu. Is the infrastructure at all locations used for the processing and storage of client data housed in a physically secure environment?

Offices are locked and only specifically authorised personnel given keys. All employees are made aware of who does have access to given office areas.

Password protected user accounts and user session time-outs happen automatically with workstation locking are implemented to mitigate against casual, opportunist or accidental breaches of data. Computers not needed online after hours follow auto-shutdown policy.

Qu. What system(s) of physical access control to the secure environment is deployed e.g. swipe cards, PIN code, and biometric readers?

Three layers of password protection (BIOS, OS, VM guest OS), obscure access to the VM used to access client systems and interactive terminals needing physical presence.

Qu. Are all accesses logged and retained with the individual's details and a time and date stamp?

Two layers of logging access to the machine (OS and VM guest OS) are employed and retained indefinitely.

Qu. Is this asset or infrastructure and locations protected against:

- Loss of power?
- Fire?
- Flood?
- Temperature?
- Humidity?

Please provide details.

- System in question is protected against:
- fire by being housed in a building protected by fire alarm which is
- tested weekly by a third party
- temperature by automatic heat monitoring and overheating protection software

Qu. Are off-site data backup storage facilities used? If yes, what physical security measures are in place and how is access controlled?

Off-site backups are stored, controlled and accessed only by selected employees and supervised by Technical Director with storage at an off-site location.

Qu. Is this asset or infrastructure hosted or located at a site managed by a 3rd party?

No

Internet, Network, System and Application Security

Qu. Please provide details of internet connectivity and associated architecture within your company.

Fibre optic Internet connection is shared between all workstations in the office and comes through a hardware router which also serves as a first step firewall solution protecting internal infrastructure from outside threats.

Qu. Are applications developed in line with principles such as the Security Development Lifecycle to safeguard against fundamental application vulnerabilities?

Graphical Data follows industry standard best practices when developing software both for security and maintainability. Graphical Data adhere to our own policies for secure software which cover data accepting, processing and handling, secure user authentication and session fixation.

Qu. Do you undertake any active vulnerability scanning of your internal infrastructure (e.g. Operating Systems, Databases, and Applications)? If yes, please give details including remediation.

Our systems are set up to receive vendor or solution provider updates as soon as they become available.

Qu. How is remote access securely managed? Who is granted remote access and how?

Graphical Data does not operate remote access method to it's internal network.

Qu. Are operating systems, databases, and applications hardened to a standard build configuration?

Yes except operating systems on employee machines. Graphical Data adhere to best security practices when it comes to hardening our infrastructure.

Qu. What is your security patch management strategy? Please describe your approach and the controls applied.

Security patches are applied depending on their purpose: external libraries used/linked are updated when their relevant patches become available and are approved by the library owner/community operating systems are updated as soon as a patch becomes available from the vendor (Mac OSX and Windows) otherwise subcomponents are updated daily (Linux) updates to Graphical Data software are developed and applied as soon as a vulnerability is found and a patch ready. Code security takes priority over functionality fixes.

Qu. Does your organisation have a formal Change and Release Control process thatrequires approvals?

Graphical Data operate a process for changes, including:

1. Identify and Raise Request for Change
2. Request is evaluated and assessed by appropriate personnel
3. Change is either rejected or authorised.
4. If authorised, change will be implemented, tested and released.

Throughout the process all requests are recorded and stored.

Qu. Are changes and releases vetted for security vulnerabilities?

One of the steps involved during Change Request evaluation is to verify that no data, internal structure or protected piece of the architecture will be exposed if requested change were to be implemented. Failing to meet these criteria will cause the Change Request to be rejected and reasons for it communicated back to the party proposing the change.

Qu. Does your organisation have separate test and production environments?

Yes. Test/development environment is set up behind firewalls on an internal server accessible only internally in Graphical Data premises. Production environments are provided by clients.

Access Control

Qu. Who will have access to client data (in all environments, e.g. test, UAT, production etc)? Please describe by function (vendors, customers, end customers, partners, operational support, developers etc.)

For up to date information, please contact info@graphicaldata.co.uk

Qu. How will this access be audited?

There will only be one dedicated machine used to access Client network externally and access to that machine will be logged (timestamped) and audited as described

Qu. Will this audit data be available to client?

Yes if required

Qu. Does your organisation allow “all powerful” or high privileged accounts on the system? If yes, how many people hold such an account? How is this controlled? Please provide details.

Yes, only Technical Director will hold such privilege.

Qu. Is there a formal process for granting, enabling, requesting, authorising, monitoring and deleting access to client data?

Considering the size of our organisation, we do not feel a complex process is necessary. Graphical Data do, however, have standards for maintaining the list of User Roles and Account profiles, processing access requests and ensuring all permissions and users are kept up to date.

Disaster Recovery

Qu. Please describe your disaster recovery procedure or processes:

In case of a disaster first step is to try resolving the issue locally, in Graphical Data office.

If for any reason this is not feasible or would take longer than 1 hour all operations are taken to a secondary location with redundant infrastructure and work restarted as normal. At the same time all necessary steps are taken to bring our primary work location back to operational state.

Qu. What are the recovery timescales?

In respect of services to clients, our recovery time target is to be no greater than 6 hours.

Qu. Has this process been tested recently (last 12 months)?

Yes, Annually – and successfully.

For up to date information, please contact info@graphicaldata.co.uk

Technical / Operational Support

Qu. Please provide details (including internal and external Service Level Agreements) of the technical / operational support services available to your employees engaged in servicing the proposed contract

Graphical Data does not currently require any external service in order to support client.

Technical Asset / Infrastructure

See separate documentation on latest build and configuration.