Web Based Hosting Security & Frequently Asked Questions

1. How many hosting company employees can access client data and how is this access provisioned, monitored and removed?

The Effective system is hosted by Protocol Internet Technologies Limited (PIC). PIC has 7 dedicated Technical Support employees who would potentially have access to the hosting server. Access is via SSH and also the Xen VPS console. Access is required for server software updates and maintenance. Outside of scheduled tasks access to the server is undertaken on a ticket-only permission basis. Access is logged to Centos SSH logs, and summary of access is emailed to our software engineer on a daily basis. These logs are routinely audited for any irregularities and for comparison against tickets raised.

2. What physical controls ensure the security of the computers used by employees of the hosting company to access hosted applications and/or data?

The Application is hosted on a VPS. The VPS resides on physical servers located in the Interxion Data Centre, Dublin. Access to servers requires Eyes & Ears authorisation, with cabinets normally locked and requires data centre security clearance. PIC also require user passwords for each PC, running industry grade anti-virus (Nod32) and permit only authorised staff to have access to their offices.

3. What is the password policy? How will passwords be communicated to users?

Users are sent an email with a 1-time activation code. This code and email combination allows the user to specify a password, at which time the activation code is obsoleted. The Application does not store the password, but rather stores a hash code from the password, which is used for future password comparisons. Lost passwords cannot be recovered, and account recovery results in a new activation code, with the entire process beginning afresh.

4. What is the authentication process for users?

Authentication is a combination of user id (email address) and password - no external devices are required. All accounts on the Application are specific to the application, and are not shared with other systems.

5. ***Will the connection to the hosting service be point-to-point or over the public Internet? How will the connection be encrypted?***

User connection to the Application will be across public Internet. All connections to the Application use 2048-bit SSL (https) connections. Application is set to respond on port 80 and port 443. All requests to port 80 are redirected to 443 (https). All connections are from the User / Client Company to the Application - the Application does NOT require connection to the user / client systems.

EffectiveSoftware
Guinness Enterprise Centre, Taylors Lane, Dublin 8, Ireland
Tel: +353 (0) 1 4853551 | **Email** support@effective-software.ie
Web: www.effective-software.com

Web Based Hosting Security & Frequently Asked Questions

6. How is the hosted data protected for unauthorised access by external parties?

The Application resides on a Centos VPS. PIC operates and monitors Cisco public-facing firewalls and in addition, Centos IPTables configures an on-system firewall to limit access from network peers.
Specific users of Effective software have requested access for routine testing of the system and hosting firewalls. These are scheduled security checks running every weekend to highlight any potential vulnerability with actions arising where necessary. Details of customers currently conducting these scans can be provided upon request and with agreement of the users in question.

7. What arrangements are in place for resilience of service? What service level is provided as standard? What disaster recovery provisions are there?

The data centre infrastructure includes redundant power supplies, networks (ports, switches, firewall and carriers) and RAID5 disk arrays. The working database is snapshot once every hour on the VPS. All uploaded attachments are further uploaded to Amazon AWS S3 (Europe Zone: Dublin) with 99.999999999% storage guarantees (Amazon documentation referenced in section 4). We complete a full server nightly backup to Amazon AWS. We provide a standard 4-hour response time with disaster recovery testing showing resumption of service within 2 hours on engineering machines (equivalent to new environment)

8. Are appropriate processes in place at the hosting company to ensure that external data regulations are complied with?

Effective Software (BCD Safety & Business Support T/A Effective Software) and its required agents are registered with the Data Protection Commission in Ireland (http://www.dataprotection.ie). We do not store or process any financial data; Client Administrators will have full control over who within the company can access each module and the relevant contained data.

9. Is there any security certification in place?

The Interxion Data Centre where the physical servers reside is ISO 27000 accredited. Although we do not hold financial information we are currently implementing a PCI-DSS SAQ (Assessment D – Service Providers) compliance process, part of which will involve regular (quarterly) security scanning from an Approved Scanning Vendor (Comodo Hacker Guardian).

10. What Capacity Planning is in place?

It is Effective Software policy to continually monitor system usage and ensure that adequate future provision is made based on usage history and expected patterns. Future planning is undertaken to ensure that hardware provision is available for continued expansion. We operate on a continual improvement basis and upgrades to system architecture to make better use of available hardware are always considered.

Web Based Hosting Security & Frequently Asked Questions

11. Access Control

The client will have full control over internal access levels. This will initial reside with the super user but also to any administrator granted "Admin" access token. Each Access Level (visible by user) can be reviewed by Admin. Automatic deletion of active access levels are in place for users marked as "Has Left" on the Organisational Chart, these users will be visible in the employee archive. Each access module can be accessed as either a read-only view or as an admin with any combination of read / write access possible by system administrators.

Other points to note in relation to Access Control:

- Session timeout is timed at 20minutes with login process returning you to the same page/state as logged out to minimise WIP data loss.
- Limitation of use by time is not in place but could be facilitated if necessary
- Definition and level of access tokens (read / write) could be redefined upon setup if necessary
- Three failed login attempts results in a 15min lockout for that user. Again not currently in place but automatic notifications could be implemented when this occurs to designated administrators.
- Once decided the system URL should be white listed for all applicable BG-Group sites

External References

Protocol Internet Technologies
Privacy Policy: http://www.hostingireland.ie/privacy-policy.php
T&C: http://www.hostingireland.ie/termsandconditions.php

Amazon S3
SLA: http://aws.amazon.com/s3-sla/
Privacy Policy: http://aws.amazon.com/privacy/

Interxion Data Centre
http://www.interxion.com/