Vendor Exchange Security | Technical Clarifications

1. Who in Portalink has access to your data?
    - Implementation (support) team
    - Technical team
    - These are all direct employees of Portalink. Access to servers is closely monitored.
    - All employees are bound by a strict code of conduct and confidentiality clauses.

2. Security standards that Portalink and its development process are certified against?
    - Portalink uses Agile Software Methodology, specifically Scrum for our product development/features and Kanban for our Support tasks. Our technical team adhere to industry standard agile development practises. Some of which include: a strict coding standard, a standard source repository branching policy, continuous integration, pair programming and peer reviews.

3. Security standards the hosting provider is certified against.
    - Our hosting provider is Amazon AWS.
    - Please see http://aws.amazon.com/compliance/ for details.

4. Is financial information such as credit card or bank accounts details stored in your application?
    - No, no such information is stored in our application.

5. Portalink's independent security auditing process.
    - We rely on the Amazon security audit process.
    - Please refer to http://aws.amazon.com/compliance/.

6. Portalink's patching and vulnerability management strategy.
    - **Application:** We schedule routine checks of library versions used in our application. When updated versions are available (due to security issues resolved or general performance and bug fixes), we confirm they are backward compatible, apply the new libraries and test.
    - **Infrastructure:** We use the Amazon Linux AMI's. The configuration of these enhances security by focusing on two main security goals: limiting access and reducing software vulnerabilities. The Amazon Linux AMI limits remote access capabilities by using SSH key pairs and by disabling remote root login. Additionally, the Amazon Linux AMI reduces the number of non-critical packages, which are installed on our instances, limiting our exposure to potential security vulnerabilities. Security updates rated "critical" or "important" are automatically applied on the initial boot of the AMI. Upon login, the Message of the Day (*/etc/motd*) indicates whether or not any additional updates are available.

7. Portalink's security incident handling process
    - Whenever a security incident becomes known (helped by monitoring the Amazon AMI Security Centre at https://alas.aws.amazon.com/), a general alert is sent to all staff and the issue is immediately escalated to our senior technical staff. They analyse the issue and determine the best course of action and inform our management team about the issue and recommended a course of action. Once approved we prepare an action plan. We use a tool called Jira to track all of the activities required to resolve the issue. We also notify customers (and our staff) about any required maintenance event and post the event on our internal calendar. We provide 24/7 technical support to our clients. Should any breach ever occur, Portalink Technical Support will mitigate the risk and will alert the impacted clients in the earliest possible timeframe.

8. Portalink does enforce secure communications channels for all external communications.

9. SSL Certificates: Portalink use certificates provided by GlobalSign and Symantec, both are well-known certificate providers. The certificate meets industry standards for security.

10. All data flows used by the Portalink system are encrypted.

11. Monitoring and protect against threats to our services.
    - Our logs are monitored for unusual/unwanted activity and an IP blacklist is maintained blocking unwanted request activity. For further details please refer to http://aws.amazon.com/security/

12. The encryption used to protect your data while it resides on the Portalink System.
    - Yes, we encrypt our Amazon RDS instances.
    - We use the Amazon Key Management Service (http://docs.aws.amazon.com/kms/latest/developerguide/overview.html) to manage all keys.

13. Password storage method.
    - Passwords are stored in a database in hashed form (no plain password is stored). Passwords are hashed using a combination of MD5 and Base64 Encoding.

14. Portalink does ensure that passwords are sufficiently complex.
    - The system enforces strong passwords (a combination of a mandatory minimum of 6 alpha-numeric and special characters).

15. The lifecycle of a user's session and the safeguards in place to prevent session hijacking or another misuse.
    Custom session management is implemented. The session is destroyed automatically when web-browser gets to be closed or after a configurable period of inactivity

16. Penetration Testing: Portalink performs vulnerability scanning and penetration testing annually.

17. Methods of authentication.
    - Username/Password

18. Control of user's access to application functions.
    - User Roles and User Privileges

19. Logging of access and usage available.
    - Can be configured as required

20. Entities and locations involved in the hosting, processing and administration of your information in the Portalink system.
    - AWS allows for different regions across the world for hosting infrastructure.

21. The platforms, development technologies and frameworks are used by Portalink.
    - Apache HTTP Server, Tomcat WebServer, MySQL, Java, Hibernate.

22. Web browsers that are supported.
    - Google Chrome, Safari, Firefox and Internet Explorer (version 9 and above).

23. No web browser plugins or extensions required? For example; Adobe Flash, Java VM, Silverlight

24. Mobile platforms supported by the Portalink System.
    - Any web-enabled tablet capable of browsing the internet, including the iPad.
    - Responsive screen display.

25. How is Portalink engineered to meet targeted service levels?
    - We over-engineer the capacity. Our servers have ample RAM and CPU. Our servers run at a low CPU usage, even during peak times the "load" is much less than capacity. We use Amazon Load Balancing to distribute requests across multiple services. These services are all part of an autoscaling group that increases the instances as load increases.

26. Portalink Disaster Recovery plan?
    - All data is stored on Amazon S3 and Amazon RDS (depending on the type and requirements of the data). S3 is designed to provide 99.999999999% durability, so for example, if you store 10,000 objects with Amazon S3, you can on average expect to incur a loss of a single object once every 10,000,000 years. (see http://aws.amazon.com/s3/faqs/#Data_Protection for further details).

    - Our RDS are configured for Multi A-Z deployments, it provides synchronous replication to a slave server in a different zone and will automatically failover in case of failure on the primary (see http://aws.amazon.com/rds/details/multi-az/#Benefits for further details).

- Our services are run behind a Load Balancer and are part of an auto scaling group. The system is configured to always have a minimum number of services running and if during any failure the instances go offline, new instances are automatically started up.

27. Backup of Portalink System
    - A full backup is performed daily, and transaction logs are saved as updates are performed. We retain the backups for up to seven days.
    - There is no additional cost for data retrieval

28. Data restoration options available to your company in the event of 1) Accidental deletion or modification of a single piece of critical information. 2) Rollback of the entire system to a point in time.
    - 1) Our standard policy is to not delete but archive data where applicable, this enables to recover any single piece of critical information.
    - 2) We can restore to any point in time up to a maximum of seven days

29. Data Access: Portalink has access to the data set that is made available to us via flat files by the clients e.g. Rich Product Data/Contract Pricing/Vendor information. The information is stored in Portalink's Database. We access our systems in AWS via private key. We do not use passwords to access our systems.