Feedback Ferret

Security Addendum

Document Reference	Feedback Ferret – Security Addendum
Version	3.0
Date Created	June 2013
Effective From	20 June 2013
Issued By	Feedback Ferret – Systems
Changed History	Reviewed – June 2016
Enquiry Point	Mark Spicer Technical Director Feedback Ferret Limited 22 Wycombe End Beaconsfield HP9 1NB United Kingdom Tel: +44 (0) 1628 681 088 Email: mark.spicer@feedbackferret.com

Table of Contents

Purpose of this Document

Feedback Ferret (hereinafter referred to as "the company") takes the threat of security breaches very seriously and is committed to understanding and minimizing risks associated with those threats.

This document should be read in conjunction with the following documents:

- Feedback Ferret – Corporate Security Policies
- Feedback Ferret - Breach Response and Security Incident Response Plans

It provides additional security information concerning the company's technical platform.

Technical Platform

The company utilizes various technical platforms to manage the entire Customer Feedback Management and Customer Experience Management processes from end to end.

We made the decision some years ago to move away from a traditional client server environment running on costly Microsoft platforms to less costly and more flexible open source platform with a view to deploying our solutions using a Cloud-based paradigm.

We looked at numerous vendors but we felt the offering from the Amazon Web Service (AWS) platform (http://aws.amazon.com) was very strong technically and provided a robust security and compliance environment. AWS provides a highly scalable cloud computing platform with high availability and reliability, and the flexibility to enable us to build a wide range of applications and services for our clients. Furthermore, it is the same platform upon which Amazon run their global enterprise and this gave us the reassurance that our security demands and those of our global client base would be met and generally exceeded.

In addition, AWS provide an extensive and growing range of back-end technical services that we use as the framework for much of our enterprise solutions. It was if they were designed specifically for our use-cases and have proven to be exceptionally reliable, secure and flexible as our needs and those of our clients have grown.

Importantly, AWS enables us to host systems and services across the globe in any of the Amazon Data Centres which form their Global Infrastructure, locating data services nearer to our clients for performance, security, legal and political reasons.

Transitional Development Platform

As we moved from our old Microsoft environment to the new open source platforms, we leased server hosting facilities at a UK based service provider IOMart (http://www.iomarthosting.com) which were used primarily for systems development, and small, short-term pilot programmes. As of February 2013, this all migrated over to AWS to gain the full benefit of their managed services.

Security

AWS provides end-to-end security and end-to-end privacy. It builds services in accordance with security best practices, provides appropriate security features in those services, and documents how to use those features. As AWS customer, the company must use those features and best

practices to architect an appropriately secure application environment. This enables us to ensure the confidentiality, integrity, and availability of our customers' data, maintaining trust and confidence.

AWS provides a wide range of information regarding its IT control environment to its customers through white papers, reports, certifications, and other third-party attestations. This information assists customers in understanding the controls in place relevant to the AWS services they use and how those controls have been validated by independent auditors. This information also assists customers in their efforts to account for and to validate that controls are operating effectively in their extended IT environment.

For full details of the AWS security environment please see http://aws.amazon.com/security.

ISO 27001 Certification

AWS has gained ISO 27001 certification, demonstrating their commitment to information security at every level. Compliance with this internationally-recognized standard, validated by an independent third-party audit, confirms that their security management program is comprehensive and follows leading practices. This certification provides more clarity and assurance for customers evaluating the breadth and strength of their security practices.

Monitoring Systems

Until now we have monitored our AWS systems using traditional methods such as manual checking of server (web and database) log files, server activities and so on. Moving forward we will increasingly be using Amazon CloudWatch which provides monitoring for AWS cloud resources and the applications running on AWS. Developers and system administrators can use it to collect and track metrics, gain insight, and react immediately to keep our applications running smoothly and securely.

Amazon CloudWatch monitors AWS resources such as Amazon EC2 and Amazon RDS DB instances, and can also monitor custom metrics generated by a customer's applications and services. With Amazon CloudWatch, you gain system-wide visibility into resource utilization, application performance, and operational health.

