Footdown Cloud Security Policy

21/01/2020
Version 1.3

Introduction

This Cloud Security Policy outlines the security of Footdown's hosted cloud services and is based on the National Cyber Security Centre (NCSC) Cloud Security Principles. It is intended to provide an adequate level of assurance that Cloud Services are delivered securely meeting the minimum security requirements as stipulated by NCSC.

Cloud security policy details

<table>
<tr><th colspan="2">Data in transit protection</th></tr>
<tr><td colspan="2">User data transiting networks should be adequately protected against tampering and eavesdropping.

Footdown can assure clients that;

• Data in transit is protected between any end user device(s) and the service
• Data in transit is protected internally within the service
• Data in transit is protected between the service and other services (e.g. where APIs are exposed)</td></tr>
<tr><td>How is data protected between the end user device and the service?</td><td>SSL is used with all data communication (all connections) between the end user device and the service. We use an extended validation SSL (SHA-256, 2048-bit RSA, plus ECC).

The website implements HTTPS everywhere; uses the Strict Transport Security Header / prevents all non-SSL connections.

All URLs for the website distributed to users include the https:// portion (to avoid 'man in the middle' style attacks from a redirect).

Any cookies used are secured; SSL only, and 'SameSite' protected. Response headers revealing server technologies are removed. Response headers such as Content-Security-Policy, X-Content-Type-Options, X-Frame-Options, and X-XSS-Protection to help protect against security issues such as cross site scripting attacks.

The software & frameworks used to provide the front-end to the device are industry standard; e.g. ASP.Net MVC v5.2.5 running on Microsoft .Net 4.7.2 served from IIS8 – and using ASP.Net Identity v2.2.1 (with OWIN middleware) for login security.

ASP.Net Request Validation & Anti-Forgery validation is used to avoid malicious payloads.</td></tr>
</table>

	The server and software used are regularly updated, patched, reviewed, and monitored.
How is data protected internally within the service?	Logins are protected using Industry Standard frameworks (ASP.Net Identity with ASP.Net MVC and Entity Framework). A default login to the system only has access to the web app for answering an event (from their phones/tablets/desktop). The only data a default login can "see" is data pertaining to their own current "Events", and only their own answer data. Additional user privileges (access to other features) are granted by an administrator through our Roles & Permissions system (using at its foundation the established Microsoft ASP.Net Identity Roles system). Even if they have been granted access to additional features/screens – a user will only see on those screens the data they have been permitted to access. We have specifically built into the design features to ensure even privileged users can never see data outside of their own organisation. Our software architecture design includes a layer we term the "Inner Castle Walls" layer – sitting below the Business layer, and above the Data layer. All requests for data flow through this. It ensures any data requested by any part of the system a user's device is always checked and filtered to only the data the logged-on user is permitted to see. If a user attempts to hack a request - e.g. manipulate a URL query string, use the browser debug console to manipulate a request, or in any way attempts to load data they are not permitted to see - it will appear to that user that the requested data does not exist at all. Microsoft.Net's non-immutable SecureString is used on more sensitive in-memory data to help avoid data being exposed by e.g. examining the paging file or scanning the (managed memory) garbage collector. Encryption of configuration files, and (beyond the HTML5 front-end) deployment only of obfuscated compiled/object code. The application's design, the frameworks used (.Net/ADO.Net/Entity Framework), server configurations &

	the chosen n-tier architecture prevents data attacks such as SQL injection. Data is stored in a protected SQL Server database that is only accessible from the server itself (no external connections possible). Individuals' specific responses are protected in numerous ways to ensure anonymity; e.g. even a very privileged user can only see responses in an aggregated or anonymised fashion – and minimum response sizes (e.g. at least 5 users contributing) are enforced before any results can be viewed.
2. Asset protection and resilience	
User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure. Footdown can assure clients; • Countries in which data will be stored, processed and managed are compliant with relevant legislation e.g. Data Protection Act (DPA)	
Where is the data physically stored and backed up?	UK Based Tier 4 Data Centre. Pulsant in Maidenhead, UK. https://www.pulsant.com/services/colocation/maidenhead-datacentre/
Has the data storage facility or data centre been subject to any external audit? if yes, please describe the audit process	Pulsant state "continual internal and external audit programme against international and industry accepted standards for security, with Quarterly management review of progress against targets and metrics and the programme for ensuring employees are aligned and understand their responsibilities"
Does the data storage facility or data centre comply with any recognised security standards?	• Tier 4 standard • 24/7 security • ISO 27001 (and more - see: https://www.pulsant.com/why-us/accreditations/)
Are there any additional encryption or other methods used to protect data at rest?	We maintain a dedicated cloud server to which only we (and the hosting company) have access. We use appropriate server configuration, firewalls, access controls, malware and

	patch management. Our SQL Server is only accessible from the server itself. We have database (column-level) encryption options that can be deployed on a client by client basis if requested (i.e. if the hosting company is not themselves seen as a trusted partner by the client). They are deployed selectively as the on-demand decryption of data can notably reduce performance in some areas of the application. This uses a master key, a certificate, and a high strength symmetric key with values kept securely known only to Footdown. The accreditations of our current Hosting provider – Storm Internet Ltd – can be viewed here: https://www.storminternet.co.uk/Business-and-IT-Security-Accreditations/252 We are looking into full Transparent Data Encryption (TDE) at the database level so as to be able to offer that as standard in a performant manner. This is not available with our current version of SQL Server; however, we are considering a move to the (notably larger investment) SQL Server "Enterprise" that provides TDE out of the box (or possibly using a recognised 3rd party tool such as NetLib Encryptionizer).
How is data disposed of when it reaches the end of its life?	Data provided directly by a client organisation is deleted from our database at the request of that organisation. At present we retain historical data from all our customers allowing automated comparisons between new and historical surveys carried out by that client.
3. Separation between consumers	
A malicious or compromised user of the service should not be able to affect the service or data of another. Footdown can assure clients that; • That the service provides sufficient separation of our data and service from other users of the service • That management of our service is kept separate from other users	
What is the service model of the delivered service? (e.g IaaS, PaaS, SaaS)	SaaS

How is separation between clients is achieved?	See description above of "Inner Castle Walls" layer – specifically written to ensure separation between service consumers. Also, an extensive user rules, Roles & Permissions implementation - using at its foundation the industry standard Microsoft Identity (v2.21) authentication and authorisation system.
Has penetration testing been carried out on the service? If yes, when was the penetration testing carried out and what was the outcome?	Weekly automated server testing from various recognised configuration and low-level vulnerability scanning tools; e.g. ASP.Net-specific security analyser https://asafaweb.com Result: **Full Pass** High-Tech Bridge Web Server Security Test https://www.htbridge.com/websec Result: **A+** Security Headers (with Sophos) https://securityheaders.com Result: **A** Qualys SSL Labs https://www.ssllabs.com Result: **A**
4. Operational Security	
Footdown is operated and managed securely in order to impede, detect or prevent attacks.	
Is there a robust change management process in place?	Yes
What measures are taken to protect the service against malware?	Patched regularly. All requests to the server monitored. IIS and application configurations constantly reviewed based on latest security advice. Regular reviewing of advisory services such as Microsoft's https://www.microsoft.com/en-gb/security/ Regular scheduled and automated scans from anti-malware software. Continuous site availability monitoring (including unexpected site changes monitoring).

What effective protective monitoring is there in place?	Continuous site availability monitoring. Continuous application-process logging and monitoring. In-built features for detecting issues and notifying administrators. Regular scheduled server maintenance (updates/patches/reviews/scans) as well as retrospective checks such as regular use of Microsoft Baseline Security Analyzer
5. Personnel Security	
Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.	
Are personnel checked against any recognised security standard? If so, what standards are enforced?	Not at this time.
6. Secure Development	
Footdown has been designed and developed to identify and mitigate threats to their security.	
Does the development of software or services in your organisation comply with any security standards?	OWASP
Is Footdown software developed in a secure location?	Development takes place within in a secure building. All development machines are protected by strong passwords and/or biometric access. All drives are bit-locker encrypted. Source control is kept secure within Microsoft's Visual Studio Team Services (Team Foundation Server) and two factor authentication is enabled on all development logins. Cloud backups of development assets are encrypted before uploading.
7. Supply Chain Security	
Footdown ensures that its supply chain satisfactorily supports all of the security principles which the service claims to implement.	
How does Footdown manage risk from third party suppliers and delivery partners?	Primarily through careful partner selection and secondly though contractual agreement. These partnership agreements are reviewed and revised as necessary – e.g. such as the current increased need

	for rigorous data protection to meet GDPR compliance.
How is information is shared with or accessible by, third party suppliers	Access to information is controlled by a two-tier permission system. Firstly, any data pertaining to a client is visible only to that client, to the organisation managing that client and, where Footdown is not directly managing the client, Footdown. Secondly, within an organisation, access to data is restricted to areas relevant to an individual's operational role.
How does your Footdown verify that hardware and software used in the provision of the service is genuine	Using a trusted Hosting company, a Tier 4 data centre, and Microsoft tools to verify genuine hardware/software.
8. Secure consumer management	
Footdown make the tools available to securely manage your use of the service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, application and data.	
How are users authenticated to the service?	Login system based on Microsoft Identity (v2.21) with OWN middleware in conjunction with Microsoft ASP.Net MVC (v5.2.5) and Microsoft .Net Framework (v4.7.2). To facilitate maximum survey response numbers; standard participant (zero-privileged) accounts (only) are provided with an expiring and encrypted instantaneous token login via a URL (which identifies them and the event). This only provides them with access to the survey response app (no administrative screens). Users with any system privileges at all (beyond standard participant) will always be forced to login using their username and strong password (even if they had a valid token URL).
How are user credentials protected?	Standard Microsoft Identity framework implementation.
How are user identities verified?	Username (email address) and strong password via the Microsoft Identity framework
How are privileged administrative accounts secured?	Internal permission system as described in 8 above.
9. Identity and Authentication	
All access to service interfaces should be constrained to authenticated and authorised individuals.	

What is the password policy for the service?	Passwords are system generated, are 'strong' and are not accessible or viewable via system interfaces. Generated password 'click-links' for a survey, distributed by email invitation to participants, are only active for a specific period against that specific survey. Users may update their own password ensuring additional security.
Does Footdown support two factor authentication?	No, but it is planned to be rolled out this year.
Does Footdown employ certificate based authentication?	No.
10. External Interface Protection	
All external or untrusted interfaces of the service should be identified and appropriately defended.	
Are all eternal interfaces subject to penetration testing?	See "Has penetration testing been carried out on the service?"
Was the architecture designed or reviewed by a qualified security architect?	Service architecture designed by an IT professional with 22 years' experience in software development, 6 years' working for a "Big 5" IT Consultancy (KPMG Consulting), who has architected n-tier, SOA, and Smart Client solutions (in typically Microsoft .Net, SQL Server, and HTML5) for multiple Investment Banking, Government, and blue-chip organisations – including Citi, Barclays, Fujitsu, and DEFRA.
11. Secure Service Administration	
Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.	
Does your organisation have a dedicated in-house security team?	No
Please describe your security incident management process?	Informal at present. Footdown has, as yet, experienced no security incidents.
Please describe how the system or service is administered. See https://www.ncsc.gov.uk/guidance/systems-administration-architectures for further guidance	Direct service administration using a strong password plus access permission by individual's role.

12. Secure Use of the service by the Consumer	
The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.	
Is access to Footdown restricted to authorised devices only?	No.
Does Footdown identify mobile devices or smartphones which access the service?	No (other than via username & passwords). With the front-end being browser-based (HTML5) there are limitations (imposed by the mobile device's browser) on identifying devices beyond basic information.