Better Impact I.T. Information Sheet

1 July 2019

Notes

This document is a compilation of questions we have been asked by clients or potential clients to help them determine whether or not our software was a good fit for their organization. Given the increasing number of organisations requesting the completion of custom IT questionnaires, we are hopeful that this document will address these research needs in most cases. Where it does not, we are happy to fill in custom questionnaires, but fees for this service will need to apply for implementations where the annual fees are estimated to be under £2,500.

Questions regarding the information here can be directed to tony@betterimpact.co.uk.

Table of Contents

Application

Architecture	Multitenant SaaS
Data segregation	Each user is identified by a unique username which they use in conjunction with a password for login purposes. Internally the user is assigned a unique numerical ID used as a primary database key. Access to shared information is restricted by the use of joins against the primary user field to ensure the user has access only to appropriate records. Data security profiles are handled directly in the database in addition to the Business Logic Layer which exposes data services to the UI Layer.
Development tools	ASP.NET MVC 3/4, VB.NET, JQuery/ JQuery mobile / JSON / Ajax, JQuery mobile, NHibernate
Development personnel	All internal (no subcontracting)
Integrity Controls	OWASP and the Microsoft Security Development Lifecycle
Major release cycle	4-5 years (12 hours downtime, typically starting around 01:00 GMT
Minor release cycle	Minor release (1 to 15 minutes downtime, typically starting around 02:00 GMT)
Highest number of concurrent users to date	>1,400

The Data Centre

Location	Live Data - Cogeco/PEER1(www.cogecopeer1.com) Toronto, Ontario, Canada Backup Data - Cogeco/PEER1 (for rapid restore if needed), Zero Fail (www.zerofail.com) Toronto, Ontario and Montreal Quebec, Canada
Video surveillance	Cameras throughout the premises and on the exterior
Network Operations Centre	24x7x365
Physical access controls	Key cards, biometric controls. single person mantrap doors
Power feed	Diesel generators supply the redundant power and there is on-site fuel storage capacity for 48 hours at full load. Generator redundancy is N+1. In the event of an outage of the main utility feed all generators will start up automatically and take over the full building load.
HVAC system	Closed Chilled water loop, Chiller Plant with Cooling Towers feeding Liebert CRAH units. On site well for redundant water.
Fire suppression	Pre-action dry pipe system
Data center certifications	CSAE4316, SOC 1 Compliant (Type 2 Report), (UTI) Tier III
Data center visits	Prearrangement through Better Impact is required

Data Protection – System

Data encrypted in transit	TLS 1.2 ECDHE RSA with AES 256bit
Password encryption at rest	One-way hashing algorithm (bcrypt) with random salting
Live data encryption at rest	256 BIT AES encryption
Backup data encryption at rest	256 BIT AES encryption
SSL certificate hashing	SHA-2
Brute force penetration lockout	Ten unsuccessful attempts within ten minutes on the same username lock out that username for 30 minutes. Your internal administrators can reset it for a user.
Intrusion Detection System	Automated with human intervention available 24x7 to prevent intrusion
Third party penetration tests	Annually – available on request
Customer penetration tests	Allowed with advance scheduling – Fees for our time may apply
Mutli-tenant date segregation	Each user is identified by a unique username which they use in conjunction with a password for login purposes. Internally the user is assigned a unique numerical ID used as a primary database key. Access to shared information is restricted by the use of joins against the primary user field to ensure the user has access only to appropriate records. Data security profiles are handled directly in the database in addition to the Business Logic Layer which exposes data services to the UI Layer.
Password requirements - Better Impact staff	Passwords must contain a minimum of 8 characters and include at least 1 uppercase, 1 lowercase, 1 numeral and 1 special character. Two factor authentication and brute force protection are also in place.
Password requirements – Organisation administrators	Passwords must contain a minimum of 8 characters and include at least 1upper case letter, lowercase letter and number. Brute force protection in place providing an additional guard against hijacking. Two factor authentication is also available as a free option.
Password requirements – Organisation constituents	Passwords must contain 6 characters. Brute force protection in place providing an additional guard against hijacking.
Periodic changes in passwords required	Not enforced - This is based on a growing body of evidence that this does not increase security and can potential reduce it. This WIRED magazine article is one of many available on the topic.
Password changes required after password resets	Required as part of the next log in after the creation of a profile by an administrator, the reset of a password by an administrator, or the automated password reset triggered by an administrative or constituent user.
Anti-virus software is - software and database servers	ESET Antivirus for Windows Server V6.5 (updated automatically)
Anti-virus software - production computers	F-Prot (updated automatically)
Anti-virus software -administration computers	Bitdefender (updated automatically)
Production and live data	Separate systems – no live data in the production environment
Permission-based identities with different levels of access to functions	Configurable
Admin user lockout after session a period of inactivity	Configurable
System login logging	Successful and unsuccessful attempts – retained for ten years.
Security patches	Critical patches are applied as issued by any vendor. Noncritical patches are applied monthly
Security breaches / loss or unauthorized disclosure of personal data since 2001 (Launch of the software)	None

Data Protection - Administration

Privacy Officer	Tony Goodrow - tony@betterimpact.co.uk
ISO27001 certification	Work in progress – Certification anticipated in Q4 2019
IOS Registration	ZA051032
IMIS policy and procedure records and communications	isms.online
Staff training on the care and handling of Personal Data and information security	A review of general best practices and key practices related to our specific environment are is administered annually. Topics include policy review and updates, compliance standards review, the importance of confidentiality policy adherence, what constitutes confidential information, and phishing and social engineering awareness.
Change management procedures for the software	• Changes considered are reviewed by the technical team • Technical team lead signs off on changes • Database and business rules programming is completed • Front end developers code as required • Automated and manual testing occur in the production environment • Users are advised of changes a week ahead of launch • System changes are uploaded to the live environment
Key administrative policies in place	• contracts of employment impose an obligation on employees to comply with data protection and confidentiality policies • criminal background checks are processed on all employees • annual staff review of documented information security policies to guide personnel in system access and security • clean desk / clear screen policy • role-based access control (RBAC) and the principle of least privilege • access to client data provided to staff on a need-to-know basis • client data sharing (not allowed) • security incident response plan • business continuity plan • client notification if we receive a request for personal information (2 business day window) • system access privileges of terminated employees revoked as a component of the employee termination process
Data breach response summary (should one every occur)	• Step 1 – Identify and contain • Step 2 – Notify all staff immediately and clients within 24 hours* • Step 3 – Investigate • Step 4 – Notify all staff and clients* • Step 5 – Implement change • Step 6 – Notify all staff and clients* *Clients will be notified via email to those listed as administrators in the system.

Resiliency and Restoration

Uptime guarantee (excluding planned maintenance)	99.95%
Historic uptime	99.997% over the past six years
System redundancies	Our system is N+1 across the entire system except the database server database server is configured as RAID10
Fail-over procedures	Replacements for all hardware are readily available within PEER1 with a 1 hour SLA. Data is backed up onsite for faster restoration if available (and on offsite for broader protection, of course).
Backups	• Full backup once per week • Incremental backup once per day • Transaction log backup once every 3 hours • 28 days retention • Full restoration tested once per quarter • Backups are for full system restoration only
RTO	3 hours
PTO	• 1 hour on hardware failure (if redundant hardware fails simultaneously) • 1 week if a portion of the data centre is destroyed but the data centre has room internally to provision a new server stack • 3 weeks if the data centre is destroyed and we need to have a new server stack provisioned in a new location

Data Portability and Destruction

Data destruction - Server	Clients have the capacity to delete all of their own data except for contact details. Upon request, we will delete all contact details except for those users who also have an association between their MyImpactPage.com profile and another Better Impact client. Their details need to be preserved for the user to use elsewhere.
Data destruction - Backups	Data deleted from the server is destructed 29 days after deletion from the server.
Client managed data export functionality	Client data is available for download at any time by the client. Relevant entities include their unique key.
Hard drive destruction	If the disc is still functioning, SQL field deletion. If the disc is no longer functioning or its use has been discontinued, there is a defined CP1 process for wiping and degaussing information. Certificates of destruction with drive serial numbers are available when applicable
API	Passive RESTful

Remote / Mobile Access

Can mobile use be restricted to Wi-Fi only?	No	(Yes for the recording of volunteer hours)
Can administrative access be restricted by IP address?	Yes	Additional fees apply
Is mobile use required to be PIN or Password protected?	Yes	
Does mobile use store any confidential information on the device?	No	
Can mobile use store any password credentials on the device?	Yes	Better Impact staff do not store system credentials on mobile devices (and require two-factor authentication). Organization constituents make their own choice.
How is mobile use deployed?		Access via a web browser
How is mobile use provisioned and de-provisioned?		Removal of credentials
Is remote secure network access employed?	Yes	VPN with no Dual -homing / split tunneling

Administrator Support

Administrative user support	• 24 x 5 via chat built into the software, email or telephone, all with a median first response time of under ten minutes. • Periodic chat and email support is available on weekends and holidays. • All support is provided by Better Impact staff.

Not supported in the software

- SSO or LDAP based credentialing
- service availability from a secondary datacenter as a backup
- account transactions logging