TECHNICAL FACT SHEET

Preface

This technical fact sheet addresses the most common security and data protection questions as well as compliance standard, backup procedures and data accessibility.

Data Protection

Data at Worklife Barometer is protected at many levels – From ensuring people cannot gain physical access to our servers to data encryption at your mobile device. We build on top of the best-in-class security practices of the Microsoft Azure Platform. Key words are:

- 24 hour monitored physical security. Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as natural environment threats.
- State of the art cyber defences. Intrusion detection and Distributed Denial of Service (DDoS). Intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools help identify and mitigate threats from both outside and inside of the data centers.
- Encrypted communications. Built-in SSL and TLS cryptography encrypts communications within and between system components and datacenters, and from the data center to end-users.

For more information see:
http://azure.microsoft.com/en-us/support/trust-center/security/

Compliance

Our data center complies with a wide set of international recognized standards including:

- ISO 27001/27002
- SOC 1/SSAE 16/ISAE 3402 and SOC 2
- United Kingdom G-Cloud
- EU Model Clauses
- Singapore MTCS Standard
- ISO/IEC 27001:2005 Audit and Certification
- Federal Risk and Authorization Management Program (FedRAMP)

For more information see:
http://azure.microsoft.com/en-us/support/trust-center/compliance/

Data Backup

Data at Worklife Barometer is always replicated at minimum two other servers in our data centers,this ensures that in the event of a hardware failure the system will automatically be able to continue on new hardware without any data loss nor downtime for the system. Furthermore, every night a backup of the data is copied to a secondary data center located in another geographical region. This ensures that the system can resume service in the unlikely event of major natural disaster.

Data Encryption

Whenever data travels – inside the data center or on the Internet – encryption is applied. We use standard TLS 4096-bit encryption between our edge-facing servers and end-user client (mobile apps and web browsers).

Access Control

Strong security measures are in place to ensure no-one gains unauthorized access to the Worklife Barometer Portal.

Information is only available on a need-to-know basis e.g. agents in a Response Center will only have access a person's journal oncea new case is opened. When the case is resolved then all access to that person's journal is revoked as well.

Mobile Websiteand Apps

End users may register their personal data though mobile apps or through a mobile-enabled website. Both systems uses email and a personal 4-digit PIN-code as authentication mechanism.

Whenever a user opens the App or Mobile Website a login promptshows. Upon successful validation of credentials, the server exchanges the provided credentials with a cryptographically signed token, which gives access to the granted resources for 60 minutes before it expires. After expiry the token becomes invalid andthe client must login again in order to obtain a new token.

These systems have a lower authentication level than e.g. the portal. This is to ease the user adoption and participation of the system. For that very same reason the system are "entry-only" systems. Below is a list of data available on these systems:

- (read only) Profile information: Name, email, phone number, company name, department
- (read only) Statistics: Total score of last 20 readingsof the persons wellbeing level (no "highly sensitive health information" is stored)
- (entry only) Health Information: Answer of health related questions(the 5 questions that regards the persons perception of: Happiness, Feeling Relaxed, Energy, Sleep and Motivation)

No health information is stored directly on themobile devices.

All communication between the systems isencrypted (SSL/TLS RSA 2048 bits)end to end.

Portal Security

The Worklife Barometer Administration Portal is used to gain access to the administrative tasks for company administrators as well as Response Team personnel for handling calls to end users.

Access to this portal is protected by a personal e-mail and password and either an OTP (One-Time Password sent over SMS) or a TOTP (Time-based One-time Password attached to a personal device).

Upon successful validation of credentials, the server exchanges the provided credentials with a cryptographically signed token, which gives access to the granted resources for 12 hours before it expires. After expiry the token becomes invalid and the client mustlogin again in order to obtain a new token.

Some actions performed in the portal may require reentry of credentials in order to complete the intended action.

All communication between the browser and Portal APIs are encrypted (SSL/TLS RSA 4096 bits) end to end.