Figlo Platform - Online Security

Title:	Figlo Platform – Online Security
Subject:	A summary of Figlo Platform security
Author(s):	Chris de Vries/ Meinard Noothoven van Goor
Version:	2 · 20-11-2014

Contents

Document History

Date	Version	Description	Author
2011-11-11	1	Initial document.	Chris de Vries
2014-11-20	2	amendments	M. Noothoven van Goor

1 Introduction

1.1 General

In this document an overview is given of the security measures taken to protect and secure client data in Figlo Platform. Most of the client data are personal data which are subject to the Dutch privacy Act, ‘Wet bescherming persoonsgegevens (WBP)’. This Privacy Act stipulates in Section 13, that appropriate technical and organizational measures should be taken to safeguard the personal data.

1.2 Figlo Platform Security on different levels in on different subjects

To protect the data appropriately a very broad range of security measures are taken.

Figlo Platform architecture is so designed that enables to secure the application and its Database. In chapter two, ‘Infrastructure and Application Architecture’ of this document further information on this subject is given.

Secondly Figlo Platform System Development and Maintenance are subject to strict procedures to guarantee the quality and therefore the security of the Software. In chapter three, ‘Figlo’s Security Rules and Procedures’ of this document further information on this subject is given.

Figlo Platform is hosted in the datacenters of Microsoft by the service MS Azure. It means that the extensive Microsoft security measures will apply to the hosting of it. In chapter four, ‘Hosting Security in Microsoft Azure’ of this document further information on this subject is given

Finally the proof of the pudding is eating and Figlo organizes a Figlo Platform security test by a third party ‘Pine digital security’ including a penetration test and code review. All Pine security recommendation will and are followed up. More information is found on https://www.pine.nl/

2 Infrastructure and Application Architecture

2.1 Infrastructure Architecture

The system architecture defines a multi-tier environment. Starting at the system level we define three tiers: Presentation tier (the interface), Application tier (the logic) and Data tier (the database services).

The reason of the multi-tier that is improves security and also scalability. A fundamental rule in the three-tier architecture is that the client tier never communicates directly with the data tier. In a three-tier model all communication must pass through the application tier which secures a controlled way of access to the stored data, and to secure service on an OS level.

Every tier it selves is designed in a most secure way. Responsibilities of a tier are implemented by layers. Per tier one or more layers can be deployed. For example the Application tier knows four layers including the service layer, business layer and data layer. All layers have their own (security) responsibilities.

2.2 Application Architecture

The Figlo solution consists of set of (web) services. Together they make up the entire solution. At the top level (User interface level), user interface services (Gui Layers) are defined. Almost every implementation of a user interface service is implemented for a specific environment. For Figlo security is managed via the so called Domain Providers system services which control every application request or submission to a business service. All security measures applicable on the application are enforced by this Domain Providers system services.

2.3 Database security

Figlo Platform employs SQL server as its database. SQL Server will be configured so that different SQL Server users (which aren‟t Windows users) have different rights to specified objects in the database. User one can have only read rights to table one and user two can have write rights as well. By implementing this architecture on forehand it is defined if a user can have read and or write access to an object in design.

To be able to access data from a database, a user must pass through two stages of authentication, one at the SQL Server level and the other at the database level. These two stages are implemented using Logins names and User accounts respectively. A valid login is required to connect to SQL Server and a valid user account is required to access a database.

Besides this Figlo employs the SQL Server security best practices that are edited by Microsoft. (http://msdn.microsoft.com/en-us/library/bb283235.aspx)

2.4 Access security

Figlo implements the latest security technology to safeguard its software. It is built on top of the so called '.NET Framework security stack'. The .NET Framework provides a security mechanism called code access security to help protect computer systems from malicious mobile code, to allow code from unknown origins to run with protection and to help prevent trusted code from intentionally or accidentally compromising security. Code access security enables code to be trusted to varying degrees depending on where the code originates and on other aspects of the code's identity.
Figlo employs an SSL connection with a certificate (1024bit public RSA key) which enforces a high-grade encryption (RC4 128bit) to secure connections between client and server. In 2015 it will be replaced by a 2048bit public RSA key). More information is available
http://msdn.microsoft.com/en-us/library/c5tk9z76(v=vs.110).aspx

3 Figlo's Security Rules and Procedures

3.1 Infrastructure Architecture

Figlo has adopted the ISO IEC 27001 and ISO IEC 27002 standard. The basic objective of these standards is to help establish and maintain an effective information management system, using a continual improvement approach.

3.2 ISO 27001 standard

The ISO 27001 standard was published in October 2005, essentially replacing the old BS7799-2 standard. It is the specification for ISMS, Information Security Management System.
The objective of the standard itself is to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System".
Regarding its adoption, this should be a strategic decision. Further, "The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the process employed and the size and structure of the organization".
The standard defines its 'process approach' as "The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management". It employs the PDCA, Plan-Do-Check-Act model to structure the processes, and reflects the principles set out in the OECG guidelines (see oecd.org)

3.3 ISO 27002 standard

The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001.
The standard "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization". The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of "organizational security standards and effective security management practices and to help build confidence in inter-organizational activities".

3.4 Procedures

To maintain the security policy, Figlo has to maintain security measurements on a broad scale of different fields of subjects. To cover the all area of information protection Figlo has introduced procedures conform the ISO 27002 standard procedures on the following subjects:

- Security Policy
- Corporate Security Management
- Organizational Asset Management
- Human resource Management
- Physical and Environmental Security Management

- Communication and Operations Management
- Information Access Control Management
- System Development and Maintenance
- Information Security Incident Management
- Business Continuity Management

3.5 Information Access Control Management

One important aspect of the above mentioned items: Figlo maintains the following rules and processes for ‘Information Access Control Management’:

- Physical access to the data center
- Remote access to these servers
- Access to the website / application (browsing)
- Firewall datacenter
- Virus Protection
- Reading logs

3.6 Information Access Control Management

An aspect of well-organized security measurements is the ‘System Development and Maintenance’. Figlo maintains a strict development street with four Deployment stages. The Four stages are ‘Development’, ‘Testing’, ‘Acceptance’ and ‘Production’ (OTAP). The source code will be promoted through these stages where every transition to another stage is secured by release safety measures.

4 Hosting Security in Microsoft Azure

4.1 Figlo Platform hosting in Microsoft Azure

Figlo Platform is hosted in ‘the Cloud’ provided by Microsoft through its through its Hosting service’ Azure’. As the term ‘Cloud’ is often associated with a vague and undefined service inwhich data are at the same time everywhere and nowhere. The Microsoft Azure Cloud is very concrete where every bit of data are traceable to Datacenter and server. Microsoft uses the most extensive and sophisticated security measures which are safeguarded by different protocols and checks.

4.2 Location of the data

The application Figlo Platform and its database are primarily hosted in the Microsoft Datacenter in Amsterdam with a redundancy in the Datacenter in Dublin. It means the data will never leave the European Union.

4.3 Microsoft Certificated Compliance

Microsoft has developed an extensible compliance framework that enables it to design and build services using a single set of controls to speed up and simplify compliance across a diverse set of regulations and rapidly adapt to changes in the regulatory landscape. Microsoft has information on the following specific compliance programs that applies to Microsoft hosting service that safeguards the Figlo Platform client data:

- ISO/IEC 27001
- SOC 1 and SOC 2 SSAE 16/ISAE 3402
- UK G-Cloud
- HIPAA BAA
- EU Model Clauses
- FedRAMP
- PCI DSS

More information is to be found on the following link: http://azure.microsoft.com/en-us/support/trust-center/compliance

4.4 Microsoft Security measures and features

Azure delivers an extensive foundation of various measures and features which secures a safe hosting environment for Figlo Platform. The following measures and features are in place to safeguard the security of the data:

- **24 hour monitored physical security.** Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.
- **Monitoring and logging.** Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts. In addition, multiple levels of monitoring, logging, and reporting are available to provide visibility to customers.

- **Patching.** Integrated deployment systems manage the distribution and installation of security patches. Customers can apply similar patch management processes for Virtual Machines deployed in Azure.
- **Antivirus/Antimalware protection.** Microsoft Antimalware is built-in to Cloud Services and can be enabled for Virtual Machines to help identify and remove viruses, spyware and other malicious software and provide real time protection. Customers can also run antimalware solutions from partners on their Virtual Machines.
- **Intrusion detection and 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 Azure.
- **Zero standing privileges.** Access to customer data by Microsoft operations and support personnel is denied by default. When granted, access is carefully managed and logged. Data center access to the systems that store customer data is strictly controlled via lock box processes.
- **Isolation.** Azure uses network isolation to prevent unwanted communications between deployments, and access controls block unauthorized users. Virtual Machines do not receive inbound traffic from the Internet unless customers configure them to do so.
- **Azure Virtual Networks.** Customers can choose to assign multiple deployments to an isolated Virtual Network and allow those deployments to communicate with each other through private IP addresses.
- **Encrypted communications.** Built-in SSL and TLS cryptography enables customers to encrypt communications within and between deployments, from Azure to on-premises datacenters, and from Azure to administrators and users.
- **Private connection.** Customers can use ExpressRoute to establish a private connection to Azure datacenters, keeping their traffic off the Internet.
- **Data encryption.** Azure offers a wide range of encryption capabilities up to AES-256, giving customers the flexibility to implement the methods that best meets their needs.
- **Identity and access.** Azure Active Directory enables customers to manage access to Azure, Office 365 and a world of other cloud apps. Multi-Factor Authentication and access monitoring offer enhanced security.

More information is to be found on the following link: http://azure.microsoft.com/en-us/support/trust-center/security/