Change request form

CR Doc no. 001-0014v1

Company:	FIVA	Captured by:	Dino Minuzzo
SRS ref:	N/A	Date captured:	1 March 2018
W/T number:		Project:	001-0014v1

Hours

Development	64	Design	n/a
PM / Testing	16	Allowance	n/a
		Total	80

CR001-014v1 Security Upgrades

This change request is to address security upgrades on the FIVA website, www.fiva.tv

The security upgrades are to address matters of DB security, encryption of data on the server in so much as to protect sensitive information and encrypt information such as the following stored within the FIVA system:

1. User date including but not limited to:
    a. Usernames - currently stored as text this needs to be encrypted
    b. Passwords (currently encrypted in the DB)
    c. Address details - currently stored as text this needs to be encrypted
    d. Travel details (stored within the VISA application) - currently stored as text this needs to be encrypted
    e. Travel documents
        i. Birth certificates
        ii. Passport document in its entirety - uploaded as a PDF, JPEG or PNG each file type needs to be encrypted
2. Passport Information
    a. Passport number - currently stored as text this needs to be encrypted
    b. Passport Photo uploads – uploaded and stored as PDF, JPEG or PNG each file type needs to be encrypted
3. Files created which are downloadable such as the created PDFs for
    a. Letters - stored as a PDF, JPEG or PNG each file type needs to be encrypted
    b. Invoices - stored as a PDF, JPEG or PNG each file type needs to be encrypted
4. Invoice Data such as:
    a. Address info which can be linked back to an applicant record
    b. Billing information of companies

Further to this the following will also be actioned as part of the upgrade:

5. 11.1 Encrypting the Web Server content – this is where images are stored, and these images contain the same information as stored in the database, which is currently password protected.
6. 11.2 One Time Pin (OTP) log in enhancement – the user will log into the platform using their user name and password, which will then initiate a process of sending an OTP via email, which will form an additional layer of security.
7. 11.3 The User will be sent an email containing the OTP to complete their log in, on the OPT email, the user will be able to click on a direct link which will assist in streamlining the OTP process.

Definitions:

05/03/2018

Date: Client signature:

“Stored as text”

This does not mean the data in the clear (openly decipherable) but if the DB was compromised or hacked the data would be interpretable.

“Encrypted”

Use methods such as SALT, PGP, LUKS and other encryption methods to obfuscate (deliberately make unreadable) data which is stored in the FIVA system that can be construed as security related.

05/03/2018

Date:

Client signature: