

Application Development Security Protocol

|  |  |
| --- | --- |
| Originating Department or Committee | Application Development |
| Author | Jide Aliu / Harry Politis |
| Policy number | 2016.ADSP-AD.R2 |
| Policy publication date | May 2016 |
| Monitoring process | * Checklist initiated at briefing stage * Checklist signed off by the Snr. and Lead Developers, and Project Manager * Automated live site release check to make sure document is included as part of solution * Tracker provided to compliance officer on monthly basis * Quarterly audit of project folders to ensure compliance |

Application Development Security Protocol

Nucleus Global is committed to ensuring that all data (personal and otherwise) are securely handled and held, and that we comply with all regulatory, contractual and legal requirements. To support this and monitor the process, this form must be completed by the Senior Developer and Project Manager at initiation of every application, and countersigned by a Lead Developer prior to release. Any deviation from the default security protocol, for example, removal of passwords must be accompanied by written confirmation from the client or otherwise authorised individual.

Application Name: Chrysalis Medical Communications

Project Lead: Stacey Everett and Dan Hutta

Project Manager: Kelsey Gouldthorpe

Application Release Date: January 2017

Job number: 5809996-49

|  |  |
| --- | --- |
| Collection of Personal Information | |
| Does the application collect personal information (if No, proceed to table “*Application Specific Information*”, if YES please continue) | Yes  No |
| Is personal information being collected? | Yes  No |
| If yes, please specify which groups of people e.g. patients, physicians  Web users of www.chrysalismedical.com | |
| What type of information is being collected? | |
| * Full Name | Yes  No |
| * Personal email address | Yes  No |
| * Mobile telephone number | Yes  No |
| * Residential telephone number | Yes  No |
| * Photograph | Yes  No |
| * Other (please specify) |  |
| Are personal data going to be transferred / shared / stored between companies or between countries? | Yes  No |
| * If yes to any of the above please provide details and written confirmation that this has been authorised |  |

|  |  |
| --- | --- |
| Data Storage | |
| Will Nucleus Global purchase/host the domain name | Yes  No |
| Is a SSL certificate needed for website | Yes  No |
| Are data stored in a secure server? | Yes  No |
| What is the geographical location of the server? Please, specify |  |
| Are there any specific server requirements (e.g. dedicated server, uptime etc.)? Please specify | AWS Cloud |
| If a copy of the data is stored outside Nucleus Global, is it in a secure environment? | Yes  No  N/A |
| * If yes, please provide details |  |
| Is there remote access to this data from outside Nucleus Global? If yes see below | Yes  No |
| * Controlled | Yes  No |
| * Limited | Yes  No |
| * Password Protected | Yes  No |
| * Conducted over an encrypted network | Yes  No |

|  |  |
| --- | --- |
| Data Security & Backup | |
| What is the level of encryption for these data and who authorised this? Please provide confirmation | SSL – Nucleus Global |
| Is there a regular back-up plan in place for these data? | Yes  No |
| Is the application behind a firewall? | Yes  No |
| If data are taken off-site on memory sticks or other removable media (USB) is it in an encrypted form? | Yes  No |
| Has a security assessment of the application and systems that service the client or handle the client’s data been performed? (Secure code reviews and/or security assessments on the application and on any significant modification, update, new version to the app prior to delivery to the client) | Yes  No |

|  |  |
| --- | --- |
| Data Monitoring | |
| What is the mechanism for reviewing user accounts and removing inactive ones or accounts belonging to people who have left the client’s organisation (please specify)? | No user account |
| Are users required to register in order to use the application? | Yes  No |
| Is there a method for users to unsubscribe from the application? | Yes  No |
| Is there an email or a telephone number for users to request to be unsubscribed from the application? | Yes  No |
| * If yes, please provide details |  |
| Have users who access personal data been given a unique username? | Yes  No |
| Have users who access personal data been given passwords with complexity requirements in line with the client’ security policy and or NG policy? | Yes  No |
| * Please specify level of complexity | Please specify |

|  |  |
| --- | --- |
| Application Specific Information | |
| Has a privacy statement been applied to the application? | Yes  No |
| Has a disclaimer been associated with the application? | Yes  No |
| * If yes, please specify | Please specify |
| Are there cookies used or any other tracking technology? | Yes  No |
| * If yes, please specify | Google Analytics |
| Has the application been safeguarded against directory listing, hot linking? | Yes  No |
| Are there any security measures to ensure all pages of the [website/app] are not indexed in search results (e.g. robots.txt file)? | Yes  No |
| Has the application been safeguarded against attacks? (URL interpretation attacks, input validation attacks, SQL injection attacks, impersonation attacks, Buffer overflow attacks)? | Yes No |
| Are there any open source elements within the application that requires a GNU license? | Yes  No |
| * If yes, please specify | Please specify |
| Are any/all of the components of the application the IP of Nucleus Global? | Yes  No |
| * If yes, please specify | Please specify |

To be completed by all signatories prior to release of application

**Senior Developer**

Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Project Manager**

Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Lead Developer**

Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_