# SmarterSoft Platform v7.5

## Data Security Controls, Measures & Policies

**Prepared for:**

Distribution to clients and project partners

This document contains the list of over 80 separate data security features, controls, measures and policies in place within the SmarterSoft Platform

**November 2018**


**SmarterSoft**

**Level 14, 309 Kent Street Sydney NSW 2000**

www.smartersoft.com.au

info@smartersoft.com.au

1300 66 12 88


smartersoft

work smarter, not harder

Areanet Pty Ltd trading as SmarterSoft

# Contents

# 1 Authentication

Items related to the secure identification and access of users of the SmarterSoft Platform:

1. One-way encrypted (hashed) passwords
2. Two (2) factor authentication via SMS i.e. Multi Factor Authentication*
3. Enforce password & login minimum lengths*
4. Enforce password settings (e.g. alpanum, alphacase etc.)*
5. Enforce case sensitive login names and passwords*
6. Disallow users from entering in the same password as their last*
7. Check for same login and password*
8. Group-based enforcing of password expiry / rotation after n days*
9. Force login after a password change*
10. Forced acceptance of usage policy at login*
11. System wide IP address whitelist*
12. Security group based IP address whitelist*
13. Brute force protection: User account ban after a number of failed attempts*
14. Brute force protection: IP ban after a number of failed attempts*
15. Logging of IP addresses with failed login attempts
16. Logging of user accounts with failed login attempts
17. IP ban lockouts can be FULL site or LOGIN only restricted*
18. Configurable login failed feedback messages not to give away any details*
19. Force users to change their passwords at any time*
20. Switch any user account to inactive*
21. New users created on administrator invitation email (instigated via system)*
22. Users can self-manage their own details and perform their own secure password resets*
23. Automatic deactivation of unused accounts*[1]

[1] Will be available on a later version of 7.5

# 2 Authorisation

Items related to the levels of access a particular authenticated user has to secured areas within the SmarterSoft Platform:

24. Role-based authorisation model via access groups (Hyper Admin & Super Admin groups exist by default) *
25. Hierarchical and granular specification of user's access rights, including separate create, read, update and delete rights assignable per data area*
26. Multiple views for administrators to manage user's access rights*
27. Administrators can create and manage their own access groups (lower than their level)*
28. Hierarchical data record filtering (based on access group)*
29. Hierarchical report data filtering (based on access group)*
30. Specify group-based session length*
31. Super Admin can impersonate other access groups*

# 3 General Application Security

Items related to "best practice" application programming techniques used in the SmarterSoft Platform:

32. SQL injection protection
33. HTML Script Injection protection
34. Cross-site scripting (XSS) protection[2]
35. Dynamic evaluation vulnerabilities protection
36. Object injection protection
37. Remote file injection protection
38. Shell injection protection
39. Media file upload content sniffing*
40. No "register globals"
41. Cookie security (HttpOnly)
42. X-Frame-Options: SAMEORIGIN

[2] Note: This is not done via the X-Content-Security-Policy HTTP header.

43. Restricted server-level information disclosure
44. Restricted application-level information disclosure (including in system feedback messages)

# 4 Auditing

Items related to the auditing of SmarterSoft Platform usage and changes to data records:

45. Audit user's logins and logouts*
46. Audit user's movements and actions through the SmarterSoft platform*
47. Audit user's changes to data records*
48. Audit records are maintained indefinitely, with an archive process
49. Audit records are locked down
50. Audit records are backed up as per the rest of the client's data backup schedule
51. Server access logging via Amazon Web Services (AWS) CloudTrail

# 5 Data Storage and Integrity

Items related to the protection and integrity of data records stored in the SmarterSoft Platform:

52. Entire data volume encryption – Amazon EBS, 256-bit key, AES-256 algorithm[3]
53. Concurrency control to protect against users editing the same record*
54. Auto-generated primary keys to ensure record uniqueness and referential integrity
55. Forced user action for create, update and delete operations (no auto-saving)

# 6 Data Transmission

Items related to the protection of data transmitted to and from the SmarterSoft Platform:

56. Secure Sockets Layer (SSL) in Apache httpd server, insecure ciphers disabled:
    a. SSLProtocol ALL -SSLv2 -SSLv3

[3] For more information visit:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html
- http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html

b. SSLCipherSuite ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS

57. Enforce SSL mode access (HTTPS)
58. Group-based session fixation (hijack) protection*
59. HTTP Strict Transport Security (HSTS)
60. Strong Secure Socket Shell (SSH), insecure ciphers disabled
61. FTPS (explicit mode, aka FTPES) supported for file transmission

# 7 Monitoring & Notifications

Items related to the monitoring and notification of SmarterSoft Platform health, exceptions and events:

62. Remote service uptime checking (from multiple geographical locations)
63. Server resource usage monitoring (memory usage & load monitoring)
64. Application-level exception management (ERROR, WARN, NOTICE)
65. Application logfiles are maintained on monthly rotation
66. Server-level monitoring exceptions are sent via email to SmarterSoft admins
67. Configurable SMS and email alerts for normal operational monitoring *
68. Client Administrators can send SMS and email notices to users *
69. Client Administrators can set notices to individual users, groups of users or all users upon login *

# 8 Server Hosting and Physical Security

SmarterSoft is an Amazon Web Services (AWS) Technology Public Sector Partner. All our solutions are hosted on AWS's cloud infrastructure. AWS is a secure, durable technology platform with industry-recognised certifications and audits, and is an approved supplier to the Australian Government[4].

Importantly:

70. All data is domiciled within Australia. We host our services on Amazon Web Services (AWS) in the Asia Pacific (Sydney) Region.

[4] More info @ http://www.asd.gov.au/infosec/irap/certified_clouds.htm

71. AWS is certified and/or has been audited to comply with: PCI DSS5 Level 1, ISO 27001[6], SOC 1[7] and SOC 2 audit reports as well as various US certifications (FISMA Moderate, FedRAMP, HIPAA).
72. AWS data centres have multiple layers of operational and physical security to ensure the integrity and safety of your data[8].
73. AWS is IRAP[9] assessed to have applicable ISM[10] controls in place relating to the processing, storage and transmission of UNCLASSIFIED (DLM) data for the Asia Pacific (Sydney) Region[11].
74. Each client's solution is deployed within its own single instance of our SmarterSoft Platform on its own EC2[12] or RDS[13] instance/s (i.e. not multi-tenanted).
75. Server access to AWS is limited to AWS's secure admin portal (HTTPS) and SSH

For more information, visit:

- http://aws.amazon.com/security/guidance/
- http://aws.amazon.com/compliance/

Please note that SmarterSoft does not itself carry any of the above certifications including PCI, ISO 27001, SOC 1, SOC 2, IRAP etc.

# 9 Server Patching, Updates & Monitoring

76. The SmarterSoft Platform utilises the LAMP stack i.e. Linux, Apache, MySQL and PHP running on top of the Amazon Linux operating system. Each of these server technologies are continuously being updated by their respective vendors, and thus there are regularly published patches and security updates. Generally, we apply a standard routine for testing and deploying these patches and updates as they become available.
77. Server-level monitoring is conducted both adhoc and continuously, including:
    - Database (MySQL) performance monitoring
    - Database (MySQL) optimisation
    - Server resource utilisation reviews (CPU, I/O, disk, memory)
    - Server health-check monitoring using Amazon Web Services (AWS) CloudWatch
    - Database backup checking

[5] Payment Card Industry Data Security Standard (International) https://www.pcisecuritystandards.org/
[6] ISO Information Security Management Systems (International) http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[7] More info @ http://en.wikipedia.org/wiki/Service_Organization_Controls (International)
[8] More info @ https://aws.amazon.com/compliance/data-center/controls/
[9] Information Security Registered Assessors Program
[10] More info @ Australian Government Information Security Manual and http://www.asd.gov.au/infosec/irap/certified_clouds.htm
[11] More info @ https://aws.amazon.com/compliance/irap/
[12] More info @ Amazon Elastic Compute Cloud (Amazon EC2)
[13] More info @ Amazon Relational Database Service (Amazon RDS)

- Long queries (SQL) review
- Error Logs review

# 10 Data Retention & Destruction

78. All client data is stored on either AWS EC2, RDS or S3[14] services. Upon a client requesting service termination, SmarterSoft shall terminate the client's AWS instances which means the data on any instance store volumes associated with those instances is deleted. Additionally, by using Entire Data Volume Encryption (Item 52), data on such volumes is irrecoverable.

    For more information, visit:

    http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html

# 11 Incident Response

79. Smartersoft has developed an Information Security Incident Response Plan (ISIRP) to implement its incident-response processes and procedures effectively, and to ensure that Smartersoft employees and contractors understand them. The intent of the ISIRP is to:

    - Define an incident,
    - Describe the process of responding to an incident,
    - Educate employees, and
    - Build awareness of security requirements.

    The ISIRP brings together and organises resources for dealing with any event that harms or threatens the security of SmarterSoft's or our client's information assets. Such an event may be a malicious code attack, an unauthorised access to information or systems, the unauthorised use of services, a denial of service attack, or a hoax. The goal is to facilitate quick and efficient response to incidents, and to limit their impact while protecting the information assets.

# 12 Availability, Backups & BC/DR Processes

Processes and plans related to Business Continuity / Disaster Recovery are configurable as per client's requirements. Disaster Recovery planning and testing can be conducted upon client's request. In general, the following exist:

80. All data entered into a SmarterSoft Platform by a client is owed by the client. SmarterSoft provides tools for client users with appropriate authorisation privileges to filter and download their data in part or in whole at any time:

[14] More info @ Amazon Simple Storage Service (S3)

c. in CSV format;

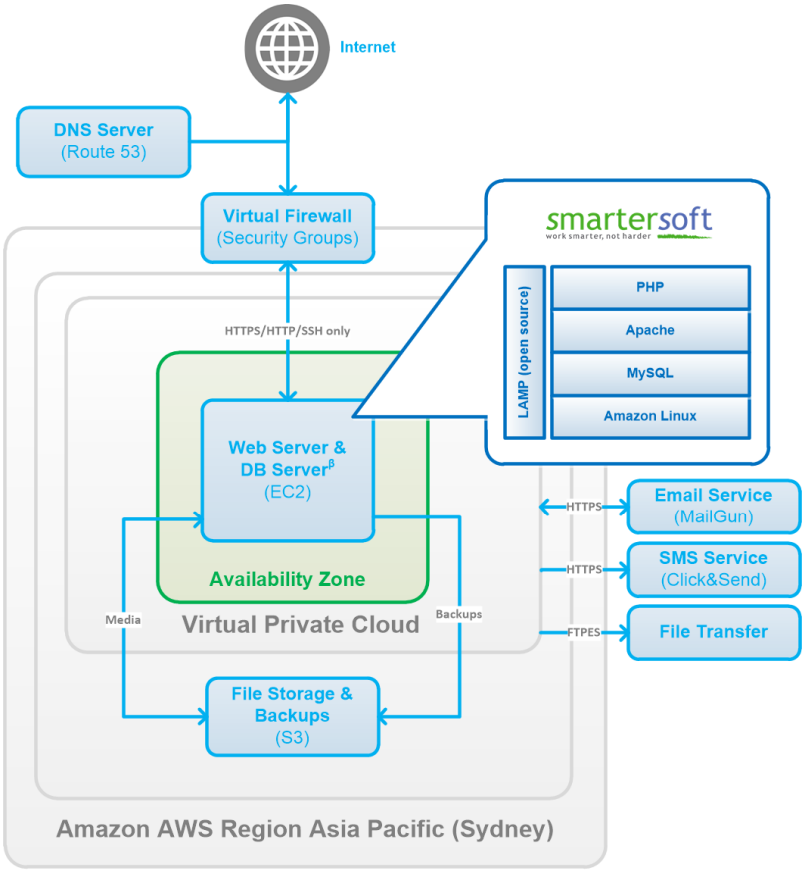
d. in XML format; including having that data transformed by XSLT (client to supply transformation file).

Clients requiring specifically formatted data may do so by request to SmarterSoft.

81. Scheduled data dumps can be configured to transfer data in CSV format to a 3rd party location via FTPeS/FTPS.
82. Metadata related to the client's database tables may be produced by request to SmarterSoft.
83. We generally offer two types of infrastructure configurations:
    - Standard Availability (manual failover, recover from scheduled backup, usually nightly)
    - High Availability (automatic failover, database replication)

## 12.1 Standard Availability Infrastructure on AWS

The SmarterSoft Platform utilises the LAMP stack i.e. Linux, Apache, MySQL and PHP[15] running on top of the Amazon Linux operating system. In the Standard Availability configuration, the Web Server and Database Server are located on the same EC2 instance with a scheduled nightly (or more frequent) database backup performed to Amazon S3. A Virtual Firewall is in place to restrict inbound TCP traffic for HTTP (port 80), HTTPS (port 443) and SSH (port 22). Separated client VPCs available on request.



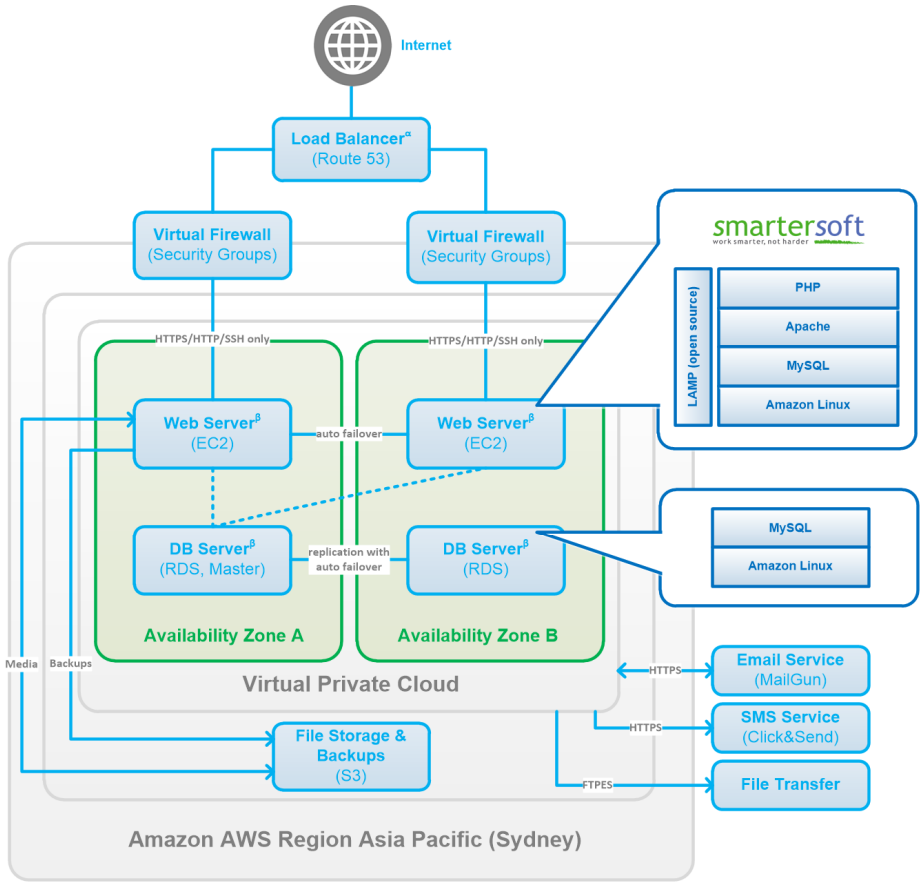

β AES 256 encryption on entire instance/volume
Server access logging via AWS CloudTrail
Sever monitoring via CloudWatch

STANDARD AVAILABILITY ARCHTECTURE

[15] The SmarterSoft platform is fully owned by SmarterSoft and is written in core PHP with minimal use of 3rd party libraries, frameworks or modules. Commercial licenses and support agreements exist for 3rd party components.

## 12.2 Higher Availability Infrastructure on AWS

The SmarterSoft Platform utilises the LAMP stack i.e. Linux, Apache, MySQL and PHP[16] running on top of the Amazon Linux operating system. In the Higher-Availability configuration, we utilise separated server instances with EC2 Web Servers "load balanced" and database replication performed via Amazon RDS. The high-availability architecture makes use of automatic failover providing near zero data loss and near zero downtime in case of failure. A Virtual Firewall is in place to restrict inbound TCP traffic for HTTP (port 80), HTTPS (port 443) and SSH (port 22). Separated client VPCs available on request.




α Requests separated using a weighted DNS routing policy with health checks
β AES 256 encryption available (on entire instance/volume)
Master DB Server may be either in A or B zone at any one time (changes on failover)
Server access logging via AWS CloudTrail
Sever monitoring via CloudWatch

HIGHER AVAILABILITY ARCHTECTURE

[16] The SmarterSoft platform is fully owned by SmarterSoft and is written in core PHP with minimal use of 3rd party libraries, frameworks or modules. Commercial licenses and support agreements exist for 3rd party components.

# 13 Privacy

84. SmarterSoft is committed to maintaining the privacy of all personal information. We publish our privacy policy at http://www.smartersoft.com.au/privacy-policy which sets out how we collect, use, disclose, store, secure, manage and access personal information in accordance with the Privacy Act 1998 and the Australian Privacy Principles (APPs). Where the SmarterSoft Platform contains personal information related to individuals on behalf of a client, SmarterSoft shall respect the privacy of those individuals by applying this policy. In such cases, individual's whose personal information is stored in the SmarterSoft Platform should also refer to each client's privacy policy for more information.

# 14 Client Responsibilities

To ensure the heightened security of the solution, all parties involved in the use and delivery of the SmarterSoft Platform must follow secure practices. Thus in addition to the data security and protection features built into the platform itself, the client also has responsibilities to ensure that they follow "best practices" on their part. At minimum the client must:

1. Ensure their staff:
    a. never give out passwords or personal login credentials to anyone
    b. never login to another user's account
2. Ensure that every single user of the SmarterSoft Platform must have their own unique login account to ensure the auditability and traceability of platform access and data record changes.
3. Ensure that all content uploaded into the SmarterSoft Platform is free from computer viruses, spyware, malware or other harmful electronic computer programs and complies with all applicable legislations, regulations, by-laws, ordinances or codes of conduct within the legal jurisdiction applicable to the client.
4. Thoroughly review and assess the sensitivity and confidentiality of the data (and media files) to be collected by and stored within the SmarterSoft Platform and notify SmarterSoft of the required security level to be hosted to. If not, we shall assume that our default level of security is applicable.
5. Ensure that the access groups and permissions feature within the SmarterSoft Platform is used appropriately such that users are not granted a level of access above their necessary usage, for example granting a standard user Super Admin access.
6. Ensure that the administrator allocated to the management of the SmarterSoft Platform:
    a. is sufficiently trained to ensure the correct creation of users and login accounts,
    b. is sufficiently trained to ensure the correct allocation of access groups and permissions,
    c. ensures the timely review and closing off of inactive user accounts,
    d. configures the platform's security settings to be in-line with their IT policies.

# 15 Support and Helpdesk Processes

Processes related to the support of the SmarterSoft Platform are configurable as per client's requirements.

In general, support is wholly managed by our online SmarterSoft Support Management System (SSMS) accessible via secure login at https://admin.smartersoft.com.au/support. One or more authorised client representatives can be given access to the SSMS to log support tasks, collaborate with SmarterSoft engineers, manage change requests, track and report on task progress, escalate tasks and view Support Block usage.

Generally, support is accessed via:

- Web https://admin.smartersoft.com.au/support
- Email support@smartersoft.com.au

* Indicates an item accessible or configurable by an authorised system administrator.