SmarterSoft Platform

Data security controls and measures

Prepared for:

Distribution to clients and project partners

This document contains the latest list of over 60 separate data security and protection controls and measures in place within the SmarterSoft Platform

Version: 3.7

Last Updated: 16th November 2016

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

1. Contents

* Indicates an item configurable by an authorised system administrator.

1 Authentication

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

1. One-way encrypted (hashed) passwords*
2. Multi Factor Authentication (MFA) via SMS*
3. Enforce password & login minimum length*
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. IP ban lockouts can be FULL site or LOGIN only restricted*
16. Configurable login failed feedback messages not to give away any details*
17. Administrators can force users to change their passwords at any time*
18. Administrators can switch any user account to inactive*
19. New users created on administrator invitation*
20. Users can self-manage their own details and perform their own password resets*

2 Authorisation

Controls related to the levels of access an authenticated user has to secured areas within the SmarterSoft Platform:

21. Group-based authorisation*
22. Granular specification of users access rights, including separate create, read, update, delete, update for approval, bulk operations and reporting rights assignable per data table*
23. Multi-level administration (Hyper Admin, Super Admin and Site Admin groups by default)
24. Multiple views for administrators to manage usage rights
25. Administrators can create and manage their own access groups (lower than their level)*
26. Multi-level data record filtering*
27. Multi-level report filtering*
28. Specify group-based session length*

3 General Application Security

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

29. SQL injection protection
30. HTML Script Injection protection
31. Cross-site scripting protection
32. Dynamic evaluation vulnerabilities protection
33. Object injection protection
34. Remote file injection protection
35. Shell injection protection
36. File upload content sniffing*
37. No "register globals"
38. Cookie security

4 Auditing

Controls related to the auditing of SmarterSoft Platform's usage and changes to data records (application level):

39. Audit user's logins and logouts*
40. Audit user's movements through the platform*
41. Audit user's changes to data records*
42. Audit records are maintained indefinitely
43. Audit records are locked down
44. Audit records are backed up as per the rest of the client's data backup schedule

5 Data Storage & Integrity

Controls related to the protection of data records stored in the SmarterSoft Platform:

45. Data volume encryption – Amazon EBS, 256-bit key, AES-256 algorithm**
46. Keep multiple versions of data records (with undo & redo)*
47. Concurrency control to protect against users editing the same record*
48. Auto-assigned and auto-generated primary keys to ensure record uniqueness and referential integrity

**For more information:

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

6 Data Transmission

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

49. Secure Sockets Layer (SSL) - protocol TLS 1.2, RSA key exchange, AES_128_GCM cipher
50. Enforce SSL mode access (HTTPS)
51. Group-based session fixation (hijack) protection*

7 Monitoring

Controls related to the monitoring and notification of SmarterSoft Platform health and exceptions:

52. Remote service uptime checking (from multiple geographical locations)
53. Server resource usage monitoring (memory usage & load monitoring)
54. Application-level exception management (ERROR, WARN, NOTICE)
55. Application exception logfiles are maintained on monthly rotation
56. Server-level monitoring exceptions are sent via email to SmarterSoft admins
57. Configurable SMS and email alerts for normal operational monitoring
58. Server access logging via Amazon Web Services (AWS) CloudTrail

8 Server Hosting and Physical Security

SmarterSoft is an Amazon Web Services (AWS) Technology Partner. All of our solutions are hosted on AWS. AWS is a secure, durable technology platform with industry-recognised certifications and audits, and is an approved supplier to the Australian Government[1].

Importantly:

59. All data is domiciled within Australia. We host our services on Amazon Web Services (AWS) in the Asia Pacific (Sydney) Region.
60. AWS is certified and/or has been audited to comply with: PCI DSS2 Level 1, ISO 270013, SOC 14 and SOC 2 audit reports as well as various US certifications (FISMA Moderate, FedRAMP, HIPAA).
61. AWS data centres have multiple layers of operational and physical security to ensure the integrity and safety of your data.
62. AWS is IRAP5 assessed to have applicable ISM6 controls in place relating to the processing, storage and transmission of UNCLASSIFIED (DLM) data for the Asia Pacific (Sydney) Region.

[1] http://www.asd.gov.au/infosec/irap/certified_clouds.htm

[2] Payment Card Industry Data Security Standard (International) https://www.pcisecuritystandards.org/

[3] ISO Information Security Management Systems (International) http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[4] More on SOC @ http://en.wikipedia.org/wiki/Service_Organization_Controls (International)

[5] Information Security Registered Assessors Program

[6] Australian Government Information Security Manual

63. Each client's solution is deployed within its own single instance of our SmarterSoft Platform on its own EC2[7] instance/s (i.e. not multi-tenanted).
64. Server access to AWS is locked down to AWS's secure admin portal (uses Google Authenticator for MFA) and SSH only.

For more information, visit:

- http://aws.amazon.com/security/guidance/
- http://aws.amazon.com/compliance/
- http://www.asd.gov.au/infosec/irap/certified_clouds.htm

9 Data Retention & Destruction

65. All client data is stored on either AWS EC2, RDS or S3 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 Data volume encryption (Item 45), data on such volumes is irrecoverable.

For more information, visit:

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

10 Availability & BC/DR Processes

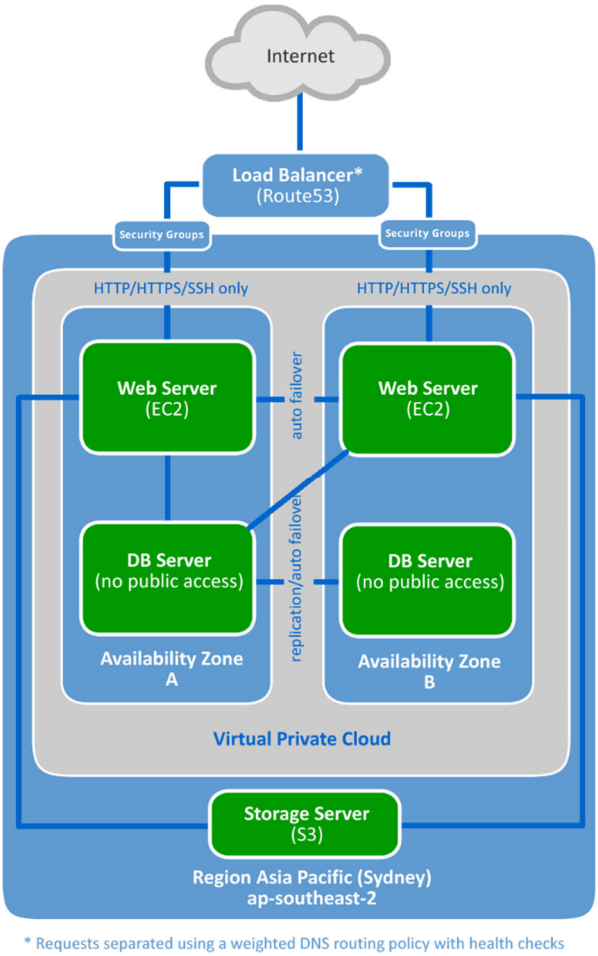
Processes and plans related to Business Continuity / Disaster Recovery are configurable as per client's requirements. Below are a few of the defaults and options available:

66. Client users with appropriate authorisation privileges may filter and download data to CSV in part or in whole at any time, or by request to SmarterSoft.
67. Scheduled data dumps can be configured to transfer data to a 3rd party location via FTP.
68. By default, a nightly data backup is performed to an alternate physical location with similar security as the production instance. Higher frequency backups are also possible.
69. High-availability options are also available on the AWS architecture which utilise geographically separated servers (web servers are "load balanced" and database replication is via Amazon RDS[8]). The high-availability architecture makes use of automatic fail-over providing near zero data loss and near zero downtime in case of failure.

SmarterSoft's High Availability Infrastructure (optional)

[7] Amazon Elastic Compute Cloud (Amazon EC2)

[8] Amazon Relational Database Service



* Requests separated using a weighted DNS routing policy with health checks

11 Support and Helpdesk Processes

Processes related to the support of the SmarterSoft Platform are configurable as per client's requirements. Generally, support is accessed via:

- Email support@smartersoft.com.au,
- Phone 1300 66 12 88
- Web http://www.smartersoft.com.au/service-request

12 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:

- Ensure their staff:
  - never give out passwords or personal login credentials to anyone

    - never login to another user's account
- Ensure that every single user of the SmarterSoft Platform must have their own unique login account to ensure the auditability and traceability of system access and data record changes.
- 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.
- Thoroughly review and assess the sensitivity and confidentiality of the data 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.
- Ensure that the administrator allocated to the management of the SmarterSoft Platform:
    - is sufficiently trained to ensure the correct creation of users and login accounts,
    - is sufficiently trained to ensure the correct allocation of access groups and privileges,
    - ensures the timely closing off of inactive accounts,
    - configures the platform's security settings to be in-line with their IT policies.