Fraud-Detection-as-a-Service for NV-DWSS (FDaaS-NV-DWSS)

System Security Plan

For the

Nevada Dept. of Welfare and Supportive Services (DWSS)

Version 1.04

December 24, 2015
## Document Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Revision Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-07-05</td>
<td>1.00</td>
<td>Initial draft.</td>
<td>Donald Carter</td>
</tr>
<tr>
<td>2015-12-24</td>
<td>1.01</td>
<td>Incorporate IRS FTI language</td>
<td>Donald Carter</td>
</tr>
<tr>
<td>2016-01-05</td>
<td>1.03</td>
<td>Feedback from DWSS</td>
<td>Edits provided to document by Robert Dehnhardt</td>
</tr>
<tr>
<td>2016-01-07</td>
<td>1.04</td>
<td>Removed HIPAA references</td>
<td>Donald Carter</td>
</tr>
</tbody>
</table>
1. SYSTEM DESCRIPTION

1.1 INFORMATION SYSTEM NAME
1.2 INFORMATION SYSTEM TYPE
1.3 BUSINESS FUNCTION
1.4 INFORMATION SYSTEM OWNER
1.5 AUTHORIZING OFFICIAL
1.6 SYSTEM BOUNDARIES
1.7 HOSTING LOCATION
1.8 SYSTEM OPERATIONAL STATUS

2. DATA CLASSIFICATION AND INTERFACES

2.1 TYPE OF CONFIDENTIAL DATA
2.2 FIPS 199 CLASSIFICATION
2.3 VOLUME OF CONFIDENTIAL DATA
2.4 INITIAL SOURCES OF DATA
2.5 POTENTIAL SOURCES OF ADDITIONAL DWSS DATA
2.6 EXTERNAL SYSTEM INTERFACES

3. RELATED REGULATIONS/LAWS/POLICIES

3.1 SECURITY REGULATIONS/POLICIES
3.2 GENERAL CONSTRAINTS

4. CONTACTS/INCIDENT RESPONSE

4.1 SECURITY ADMINISTRATION
4.2 FDaaS PRODUCT TECHNICAL SUPPORT
4.3 OTHER CONTACTS
4.4 INCIDENT RESPONSE

5. TECHNICAL ENVIRONMENT AND ARCHITECTURE

5.1 HARDWARE
5.1.1 Development Environment
5.1.2 Staging Environment
5.1.3 Production environment
5.2 SOFTWARE
5.3 NETWORK
5.4 ARCHITECTURE
5.5 SYSTEM INTERCONNECTIONS
5.5.1 From the development environment
5.5.2 From the staging environment
5.5.3 From the production environment
5.6 DATA TRANSFER
5.7 ENCRYPTION
5.8 REMOTE ACCESS

6. CONTINGENCY PLANNING

6.1 SYSTEM BACKUP
6.2 DISASTER RECOVERY PLAN .................................................................................................................. 12

7. SECURITY CERTIFICATION, MONITORING, AND OVERSIGHT .......................................................... 13
   7.1 INTRUSION DETECTION ......................................................................................................................... 14
   7.2 PENETRATION TESTING ......................................................................................................................... 14
   7.2.1 Network Level .................................................................................................................................. 14
   7.2.2 Application Level ............................................................................................................................... 14
   7.3 VULNERABILITY SCANNING ................................................................................................................ 15
   7.4 LOG MONITORING/AUDITING ............................................................................................................ 15
   7.5 RISK MANAGEMENT ............................................................................................................................. 15
   7.5.1 Risk Impact Analysis ......................................................................................................................... 15
   7.5.2 Identification of Threats and Vulnerabilities .................................................................................... 15
   7.5.3 Development of a Risk Management Plan ....................................................................................... 16
   7.6 CHANGE CONTROL AND CONFIGURATION MANAGEMENT ............................................................ 16
   7.6.1 Configuration Management: .......................................................................................................... 16
   7.6.2 Change Control: ............................................................................................................................... 16
   7.7 SOFTWARE DEVELOPMENT LIFE CYCLE SECURITY ........................................................................ 17

8. USER SECURITY ........................................................................................................................................... 18
   8.1 SECURITY AND CONFIDENTIALITY TRAINING .................................................................................. 18
   8.2 CONFIDENTIALITY AGREEMENT ......................................................................................................... 18
   8.3 PERSONNEL CONTROLS ..................................................................................................................... 18

9. AUTHENTICATION AND ACCESS CONTROL ......................................................................................... 19
   9.1 NETWORK AUTHENTICATION ............................................................................................................. 19
   9.2 APPLICATION AUTHENTICATION ......................................................................................................... 19
   9.3 ROLE BASED AUTHORIZATION MODEL ............................................................................................ 19
   9.4 ROLE BASED ACCESS CONTROL ....................................................................................................... 19
      9.4.1 Client Administrator ..................................................................................................................... 19
      9.4.2 Client User .................................................................................................................................... 19
   9.5 ACCOUNT ADMINISTRATION ............................................................................................................. 19

10. TECHNICAL SECURITY CONTROLS ..................................................................................................... 21
    10.1 ANTI-VIRUS ....................................................................................................................................... 21
    10.2 SECURITY PATCHES ........................................................................................................................... 21
    10.3 SERVER HARDENING .......................................................................................................................... 21
    10.4 WARNING BANNER ............................................................................................................................. 21
    10.5 ADMINISTRATIVE SYSTEM SESSION EXPIRATION ...................................................................... 22
    10.6 ADMINISTRATIVE PASSWORD SECURITY ...................................................................................... 22
    10.7 MEDIA DESTRUCTION ........................................................................................................................ 22
    10.8 DATABASE SECURITY .......................................................................................................................... 22
    10.9 PHYSICAL SECURITY CONTROLS .................................................................................................... 22
    10.10 OTHER SECURITY CONTROLS ....................................................................................................... 22

11. SECURITY PLAN APPROVAL .................................................................................................................. 24

ATTACHMENT A  FDAAS-NV-DWSS SYSTEM ARCHITECTURE .................................................................... 25
1. System Description

1.1 Information System Name
Fraud Detection as a Service for State of Nevada Division of Welfare and Supportive Services (FDaaS-NV-DWSS)

1.2 Information System Type
FDaaS-NV-DWSS is a major application system that performs clearly defined functions for which there are readily identifiable security considerations and needs.

1.3 Business Function
FDaaS-NV-DWSS analyzes incoming claims data from NV-DWSS systems, using Google’s predictive modeling, specialized data mining and matching, publish and subscription functionality, and search engine technologies to investigate and detect potential fraud, both pre and post payment. The system will be used by investigators, auditors and analysts.

1.4 Information System Owner
Audits and Investigations

1.5 Authorizing Official
Steve H. Fisher
Administrator
State of Nevada, Division of Welfare and Supportive Services
1470 College Parkway
Carson City, NV 89706

1.6 System Boundaries
The system boundary includes the hosting location and all security controls surrounding NV-DWSS data at the hosting location. The boundary includes all secure data interfaces which send or receive NV-DWSS data from outside the hosting location. The system boundary extends to any copies of data taken outside of the physical hosting location, such as for offsite storage, or disaster recovery sight maintenance.

Please see Appendix A – FDaaS-NV-DWSS Architecture
1.7 Hosting Location

Hosting provider Quest Managed Services and Solutions will provide the required hosting services for the NV-DWSS FDaaS computing facilities. NV-DWSS information will reside within Quest Managed Services and Solution’s data center and on Quest Managed Services and Solutions protected data servers. For additional information on Quest Managed Services and Solutions capabilities, please refer to the company website www.Queestsys.com.

In addition to exceeding the regulatory mandates listed below, Quest Managed Services and Solutions has purpose built its cloud infrastructure to uphold data sovereignty requirements in the secure cloud that does not put NV-DWSS data at risk of crossing borders. The following security capabilities are also maintained by Quest.

**PCI**

Quest Managed Services and Solutions is a certified PCI Approved Scanning Vendor.

**SSAE 16**

Quest Managed Services and Solutions SOC 1 Type 2 reports are available for review. These reports demonstrate the viability of Quest Managed Services and Solution’s control program over time.

**MASTER SERVICE PROVIDER**

Quest Managed Services and Solutions currently maintains certification as a Cisco Master Service Provider for cloud and managed services, and is a Cisco Advanced Data Center Architecture Specialized Partner.

Quest Managed Services and Solutions has reviewed the security requirements associated with the FDaaS-NV-DWSS implementation and has reported that all security requirements are addressed and accommodated within the Quest Managed Services and Solutions hosting infrastructure.

1.8 System Operational Status

System is not currently operational.
2. Data Classification and Interfaces

2.1 Type of Confidential Data

The system will use FTI, PHI and PII information that is detailed out in the data usage agreement and further detailed out in the data release documents. All Pondera employees are required to attend periodic training on the company’s Information Security Policy, and to sign an End User Information Security Policy and Proprietary Rights Agreement. An annual refresher course on all security and confidentiality policies, inclusive of the handling of FTI data, is required for all employees.

Pondera confirms that company security and privacy training includes process and procedures for handling of FTI.

2.2 FIPS 199 Classification

- Confidentiality  ➔ Medium
- Integrity  ➔ Low
- Availability  ➔ Low

2.3 Volume of Confidential Data

We estimate approximately 250,000 rows of data will be sent from NV-DWSS to the FDaaS-NV-DWSS system on a monthly basis, and 3,000,000 annually for the term of the contract.

2.4 Initial Sources of Data

The following systems are understood to provide the initial data feeds:

- NOMADS
- IRIS
- JPMorgan
- IES
- GAMMIS
- EBTAS

2.5 Potential Sources of additional DWSS Data

- Nevada will be sending a list of potential data sources.

2.6 External System Interfaces

The FDaaS-NV-DWSS system may interface with the following systems:

1. Dun & Bradstreet (Public Records)
2. Appriss Corporation (Public Records and Criminal History)
3. TLOxp Corporation (Public Records)
4. Wist / Hamari (link analysis implementation co-located with FDaaS instance)
5. Google Corporation (Maps, Fusion Tables, and Prediction APIs)
6. LexisNexis (public records, licensure records)
7. Social Intelligence (social media lookups)

However, these and/or additional systems may be added or eliminated for interface with FDaaS-DWSS upon mutual consideration and documented agreement by the project’s Authorizing Officials.
3. Related Regulations/Laws/Policies

3.1 Security Regulations/Policies

The following set of regulations, policies, and guidelines will apply to the FDaaS-NV-DWSS implementation, depending upon the data sources and data content.

- Nevada Client Security Policies and Procedures
- IRS Publication 1075
- CA SAM 5300
- Social Security Administration agreement
- Business Associate Agreement
- Data Use Agreement
- Project Purchase Order
- Nevada Confidentiality and Security Requirements for Vendors Contracts/Memoranda of Understanding (MOU)/Agreements (hereinafter referred to as NV-DWSS Attachment C)
- All constraints imposed on utilization of third-party data

3.2 General Constraints

For the sensitive and confidential data provided by or through NV-DWSS, Pondera agrees to act in accordance with NV-DWSS Attachment C. Further, Pondera agrees to sign and to have its employees, subcontractors, and agents, if any, sign and agree to provisions of NV-DWSS Attachment C.

Pondera shall use the sensitive and confidential data provided by or through NV-DWSS, only for the years specified in the purchase order and only for the purposes described in the purchase order and this security plan.

The confidentiality and security requirements for the sensitive and confidential data described in NV-DWSS Attachment C and the security plan provided by Pondera and agreed to by NV-DWSS and Pondera in writing survive the termination or expiration of the purchase order.

For personal information provided by NV-DWSS, Pondera shall not distribute for commercial purposes, sell, or rent any individual's name and address. Civ. Code 1798.60.

Pondera shall not seek to identify any applicant or recipient of social services or public assistance who may or may not be residing in a facility subject to licensure by the State of
Nevada; further, Pondera agrees not to provide any data of such individuals to NV-DWSS or the State pursuant to this purchase order, unless permitted or required by state or federal law.

In the event that Pondera receives a Public Records Act request, Pondera shall immediately within 24 hours notify NV-DWSS of such a request if it involves a request for data provided by NV-DWSS pursuant to the purchase order. In the event that NV-DWSS receives a Public Records Act request related to the data provided to or by Pondera, Pondera agrees to collaborate with NV-DWSS to respond to the PRA within the time period required by the PRA and to provide the required information if determined to be appropriate by NV-DWSS.
4. Contacts/Incident Response

4.1 Security Administration

Donald W. Carter  
Contractor – Chief Security Officer – Pondera Solutions  
Don.carter@ponderasolutions.com  
(916) 601-4398

4.2 FDaaS Product Technical Support

Tom Lucero  
Contractor – Manager Systems Development – Pondera Solutions  
Tom.Lucero@ponderasolutions.com  
(916) 531-6894

4.3 Other Contacts

NV-DWSS Personnel and Contact Information

<Insert client contact information here>

Pondera Personnel and Contact Information

Jon Coss  
Contractor - CEO – Pondera Solutions  
Jon.coss@ponderasolutions.com  
(916) 792-0205
Greg Loos  
Contractor - COO - Pondera Solutions  
Greg.loos@ponderasolutions.com  
(916) 715-3747  

Amanda Huston  
Contractor - Director of Fraud Detection and Intelligence – Pondera Solutions  
Amanda.Huston@ponderasolutions.com  
(850) 445-3851  

Asif Ahmed  
Contractor – Chief Technology Officer – Pondera Solutions  
asif.ahmed@ponderasolutions.com  
(503) 593-9414  

4.4 Incident Response  
Incident response procedures internally escalate from the Project Manager to the Pondera CSO, Donald Carter, who will work collectively with Nevada client Department personnel during incident management and post-incident mitigation activities. If the scope of the incident included Quest Managed Services and Solutions, Pondera would contact Quest Managed Services and Solutions immediately at 1-877-262-3473. The Quest Managed Services and Solutions support team is available 365 days a year (24x7). For a severity 1 issue like a security breach, Quest Managed Services and Solution’s policy is to work on the incident immediately. Our first action would be to take the Pondera servers offline to ensure no outside access to any data. Quest Managed Services and Solution’s have incident response and security procedures in place. Quest Managed Services and Solutions is currently pursuing FedRAMP compliance.
5. Technical Environment and Architecture

5.1 Hardware

A typical FDaaS service instance utilizes the following hardware configurations:

5.1.1 Development Environment

Single Virtual Host 4 cores, 24 GB memory and 2 TB of storage.

5.1.2 Staging Environment

Single Virtual Host 4 cores, 12 GB memory and 1 TB of storage.

5.1.3 Production environment

Single Virtual Host 4 cores, 24 GB memory and 1 TB of storage.

5.2 Software

FDaaS-NV-DWSS system uses following software technologies:

1. Windows Server
2. Linux Operating system
3. JavaScript programming for browser presentations
4. HTML 5
5. Microsoft .NET Framework
6. Microsoft SQL Server
7. Google Mapping APIs
8. Google Prediction APIs

5.3 Network

The Quest Managed Services and Solutions network will be configured to only allow access to port 443 (encrypted HTTPS protocol port) for client access to the FDaaS-NV-DWSS Dashboard. All access to the Quest Managed Services and Solutions servers and the FDaaS-NV-DWSS system will be over an encrypted virtual private network (VPN). A site-to-site VPN will be configured between the Quest Managed Services and Solutions network and the NV-DWSS network. NV-DWSS personnel will control access to the VPN tunnel. All Vendor support personnel will also utilize an encrypted VPN connection for all access to the environments or applications. Controlled access for SFTP file retrieval from NV-DWSS file store will be enabled on port 22.
5.4 Architecture

Please see attached FDaaS-NV-DWSS architecture diagram document in Appendix A.

5.5 System Interconnections

FDaaS uses the following system interconnections.

5.5.1 From the development environment

1. Secure FTP services
2. Dun & Bradstreet Corporation (SECURE FTP or HTTP interface, depending on size of transfer)
3. Experian Corporation (SECURE FTP or HTTP interface, depending on size of transfer)
4. TLOxp Corporation (SECURE FTP or HTTP interface, depending on size of transfer)
5. Appriss (Justice Exchange, HTTPS interface)
6. Link Analysis (Internal, co-resident service, HTTPS interface)
7. Browser side Google (for Mapping and Rendering APIs, HTTPS interface)

5.5.2 From the staging environment

1. Browser side Google (for Mapping and Rendering APIs, HTTPS interface)

5.5.3 From the production environment

1. Inbound HTTPS connections from client network.
2. Browser side Google (for Mapping and Rendering APIs, HTTPS interface)
3. FDaaS I-Frame connectivity to prescribed third-party data providers.

5.6 Data Transfer

All files, regardless of size will be posted to the NV-DWSS Secure FTP site and then downloaded via Secure FTP into the Quest Managed Services and Solutions data center transfer method, all files will be archived using either a ZIP or RAR format with 256-bit key AES encryption applied.

5.7 Encryption

The FDaaS-NV-DWSS system will use AES 256 bit based storage encryption for data at rest on all servers. Development and support systems are not permitted to store NV-DWSS data or processing results.
5.8 Remote Access

End Users are only allowed to access the FDaaS-NV-DWSS system via the FDaaS-NV-DWSS dashboard over an HTTPS (SSL) connection. There will be no other remote access to the system for the NV-DWSS End Users. Via the dashboard, authorized NV-DWSS investigators will be able to view information on persons such as Name, DOB, SSN, Gender, Address, and beneficiary claims information. Only authorized NV-DWSS staff will be able to view profile information and ‘flags’ triggered by claims information. Remote access to the FDaaS-NV-DWSS dashboard may be required such that NV-DWSS staff can review potential indications of fraud and can perform investigations.

See Section 9.5 for more details on how authorization for remote access is obtained.
6. Contingency Planning

6.1 System Backup

No physical backups are performed. The system architecture utilizes virtual backups of only the encrypted file system. The virtual backups are reused thus destroying older backups.

6.2 Disaster Recovery Plan

A Disaster Recovery Plan is not applicable as:

1. FDaaS-NV-DWSS is not a mission critical system to the operation of NV-DWSS
2. In case of disaster the FDaaS-NV-DWSS system can re-import all NV-DWSS source data and recreate the fraud analytics.
7. Security Certification, Monitoring, and Oversight

Pondera Solutions certifies that Quest Managed Services and Solutions is compliant with all security and privacy requirements for each and every FDaaS client organization inclusive of the California Department of Social Services. Quest Managed Services and Solutions offers multiple layers of security implemented both inside and outside of their infrastructure, with all pieces working together as one system. Core features of Quest Managed Services and Solutions security include:

1. Physical Security
   a. ANSI TIA-942 Tier 3 compliant data center or higher for architectural, electrical and mechanical requirements.
   b. Segregated cages, dedicated drops
   c. Multi-factor biometric access
   d. Physical access by Quest Managed Services and Solutions staff only
   e. Detailed access audit trail
   f. Security monitoring 24x7x365

2. Perimeter Security
   a. IP reputation filtering
   b. DoS/DDoS mitigation

3. Network Security
   a. Intrusion detection/prevention
   b. Unlimited isolated security zones
   c. Private network segmentation
   d. Vulnerability monitoring
   e. Vulnerability audits

4. Server Security
   a. Hardened operating systems
   b. Managed OS patches and updates
   c. Hardened VMware hypervisor
   d. Unnecessary services disabled
   e. Password security policies
   f. Malware protection
   g. Resource availability monitoring
   h. Network event logging
i. Data encryption at rest

5. Application Security

a. Web application firewalls (ports 22, 80, and 443)
b. Intelligent WAF policies for common attacks
c. Application specific and custom WAF policies
d. HTTP DoS application attack mitigation
e. Application performance monitoring
f. SSL certificates

6. Administrative Security

a. Secure remote access (SSLVPN)
b. Secure portal for user management
c. Site-to-site L2VPN
d. MPLS termination
e. Log Management
f. Two-Factor authentication

7.1 Intrusion Detection

There is NIDS installed by default and then there is a HIDS for the compliance package through the installation of OSSEC.

Quest Managed Services and Solutions does not release the vendor names without a need and right to know, but they are leading vendors within the industry space.

7.2 Penetration Testing

7.2.1 Network Level

Quest Managed Services and Solutions employs comprehensive penetration testing on an ongoing basis. Quest Managed Services and Solutions does not distribute the detailed level information of the methodology and tools as to not aid potential attackers, however, the information is available to NV-DWSS personnel with a need and right to know.

7.2.2 Application Level

FDaaS-NV-DWSS does not allow access to any of its services that can access NV-DWSS data via public internet which prevents any unintended access to any data resource. Above and beyond that, any access to any FDaaS-NV-DWSS resources are only accessible over highly secure virtual private network.
7.3 Vulnerability Scanning

Quest Managed Services and Solutions employs both internal and external scanning methods to fulfill system security scanning requirements.

7.4 Log Monitoring/Auditing

FDaaS-NV-DWSS provides comprehensive logging for all system activities including, but not limited to:

1. User system access (successful or un-successful, who and when)
2. User data access (who, what, when)
3. System administrator access and actions

_As of the time of this publication, access log retention requirements for the FDaaS-NV-DWSS system have not been identified._ As a result, no logging data has ever been purged. Access to the FDaaS-NV-DWSS system log is restricted to authorized administrative personnel. The FDaaS-NV-DWSS system provides embedded functionality to view system log entries.

Quest Managed Services and Solutions uses a number of tools that can be optimized for the customer and this is managed by the NOC. Any alerts that are created are noted by the NOC and then sent to the customer for further notification and action. In the event of unauthorized access and this is confirmed by the NOC, then any customer designated plan will be initiated and further actions taken.

All logs are available to authorized NV-DWSS representatives at any time. At the request of authorized NV-DWSS representatives, all designated and available log files will be obtained from the hosting provider, Quest Managed Services and Solutions, and presented to NV-DWSS.

7.5 Risk Management

A Risk Management Plan has been established to address the importance of information classification. The assessment is comprised of three components – Confidentiality, Integrity, and Availability.

In order to determine Confidentiality, Integrity, and Availability, all systems designs, configurations, and implementations complete the following key processes:

7.5.1 Risk Impact Analysis

The importance of all secure information assets shall be evaluated by determining the loss impact of such information assets, in order to ensure that the level of protection and resources to protect each asset is appropriate for the overall level of risk.

7.5.2 Identification of Threats and Vulnerabilities

Threats and vulnerabilities that could increase the likelihood of unauthorized disclosure, modification, or reduced availability of secure information assets shall be identified.
Controls to protect the identified assets shall be based on the identified threats and vulnerabilities.

7.5.3 Development of a Risk Management Plan

A Risk Management Plan to implement controls that mitigate risks to the confidentiality, integrity, and availability of the secure information assets shall be developed.

With each FDaaS implementation, risk assessments are performed. This occurring during the product SDLC, during the planning phase(s) for a major feature implementation, or if any of the involved data structures are being significantly altered (i.e., additional information is being stored on the system). Additionally, all systems that have not previously been assigned a risk classification shall retroactively be reviewed.

7.6 Change Control and Configuration Management

Following processes are used for Configuration Management and Change Control.

7.6.1 Configuration Management:

1. Configuration changes are submitted by NV-DWSS to the Vendor Project Manager (or designated representative) for approval. FDaaS-NV-DWSS treats new updates or changes to the existing configuration as configuration changes and follows the same process for both types of configuration modifications.

2. The Vendor Project Management team reviews the configuration for security vulnerabilities and threats and rejects the configuration if they do not meet the FDaaS security standards. This applies to both new and modified FDaaS configurations.

3. The configuration changes are designed, developed, and evaluated for vulnerabilities.

4. Results are communicated and coordinated with NV-DWSS, by the Vendor Project Manager.

5. The FDaaS-NV-DWSS System Security Plan is also reviewed for potential updates relative to the associated configuration changes.

6. Only Nevada WSS approved configuration changes will be applied to the FDaaS-NV-DWSS configuration. Nevada DWSS will provide to Pondera, a list of individuals authorized to approve configuration changes to the FDaaS-NV-DWSS instance.

7.6.2 Change Control:

1. Code changes are submitted for approval by Vendor Development staff, to the Vendor CSO. The FDaaS SDLC process treats new functionality or changes to existing code as changes and follows the same process for both types of modifications.
2. Vendor Development staff and Vendor Security team members review the application changes for security vulnerabilities and threats and reject the changes if they do not meet all security standards. This applies to both new and modified FDaaS components. The FDaaS-NV-DWSS System Security Plan is also reviewed for potential updates relative to the associated changes.

3. Only NV-DWSS approved configuration changes are implemented.

7.7 Software Development Life Cycle Security

All FDaaS software code and configurations go through above described process. Essentially all software, database components, and configurations are reviewed for security compliance before they are built, and again after all modifications are completed.
8. User Security

8.1 Security and Confidentiality Training

All Pondera employees are required to attend periodic training on the company’s Information Security Policy, and to sign an End User Information Security Policy and Proprietary Rights Agreement. An annual refresher course on all security and confidentiality policies is required for all employees. For the Nevada DWSS engagement, all Pondera personnel resources with access to Nevada DWSS data will also participate in IRS 6115-AT security training.

8.2 Confidentiality Agreement

All Pondera employees are required to sign a Confidentiality Agreement. Pondera also requires a BAA with all partners, and passes down all applicable NV-DWSS requirements to these partners.

8.3 Personnel Controls

Pondera performs background checks on all employees. Pondera also requires all employees to sign a Security Policy Acknowledgement stating the employee has read and understands all Privacy & Security Policy documents.
9. Authentication and Access Control

9.1 Network Authentication

Network access for all service support staff to the Quest Managed Services and Solutions Network utilizes two-factor authentication. Support staff use the latest Cisco encrypted VPN client to access the Quest Managed Services and Solutions environment. NV-DWSS staff utilize a methodology consistent with NV-DWSS departmental standards.

9.2 Application Authentication

Application User Authentication is handled using the industry standard ASP.NET Membership Services provided by Microsoft Corporation. The ASP.NET Membership Services manages the authentication process and integrates with credential management and application forms authorization using role based security.

9.3 Role Based Authorization Model

Authorization is handled by integrating the ASP.NET authentication with form authorization provided by Microsoft. Each user in the FDaaS-NV-DWSS system is configured into one or more specific authorization roles.

9.4 Role Based Access Control

Following are two example roles that are provided by the system. Any user can be configured with any combination of roles. If a user is not a participant in a particular role, then the associated dashboard feature is not visible to that user. At runtime, a second level check is performed to insure no unauthorized functions are accessed.

9.4.1 Client Administrator

Typically, users assigned to this role have the ability to create/remove users that will use their FDaaS-NV-DWSS dashboard. The Client Administrator role can also reset passwords for client users.

9.4.2 Client User

Typically, users assigned to this role have the ability to use the FDaaS-NV-DWSS system. They only have the ability to manage their own password and access the authorized functionality of the FDaaS-NV-DWSS dashboard.

9.5 Account Administration

FDaaS-NV-DWSS has administration functions that can be accessed by authorized users. The Client Administrator role typically will be able to add, remove, and reset passwords of users of the dashboard. To gain initial access to the administration functions, an authorized representative from NV-DWSS must contact Pondera to configure the account. Once added the Client Administrator will then have access to create new accounts with the FDaaS-NV-DWSS
system. This administration role also has the ability to disable accounts, change passwords, and modify or add roles to a given authorized user.

NV-DWSS will not approve creation of new accounts until a NV-DWSS FDaaS-NV-DWSS (Pondera) Access Authorization form (see Appendix B) has been completed, with all necessary signatures. NV-DWSS will use the same form to request termination of accounts when staff are no longer employed or have changed job roles.
10. Technical Security Controls

10.1 Anti-Virus

All systems and servers on Quest Managed Services and Solutions networks managed under this engagement, whether managed by employees or by third parties, follow this procedure:

1. All applicable systems are configured with anti-virus/anti-spyware/anti-malware software of the type specified in the information security policy.

2. The approved and prescribed software is configured to scan for viruses in real-time and log anti-virus events with routing to a central logging solution, and end users are not be able to configure or disable the software.

3. The signature updates are updated daily and as stated before, Quest Managed Services and Solutions does not distribute the name of the vendor.

10.2 Security Patches

As per requirements, the operations staff for the Quest Managed Services and Solutions NOC, lists and manages system patches received through automated alerts and then apply the patches to the customer systems within 30 days of release.

10.3 Server Hardening

There is a defined procedure that is used to harden all the servers that meets and exceeds all of the compliance standards

10.4 Warning Banner

At each login, the FDaaS dashboard presents an authorized access only warning, similar to the following. The user is required to select the checkbox acknowledging the warning message before the login button is activated.

![Pondera FDaaS Warning Banner]

Warning: This is a State of California Computer System that is for official use by authorized users and is subject to being monitored and/or restricted at any time. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you are not an authorized user or you do not agree to the conditions stated in this warning.

The Pondera FDaaS dashboard may contain certain data items governed by the Gramm-Leach-Bliley Act, 15 U.S.C. Section 6801 et seq. ("GLBA"). This data is provided to you for use under GLBA exemption which states permissible purpose as:
10.5 Administrative System Session Expiration

There are controls implemented so that all system administrative sessions to the hosted virtual machines are terminated after 15 minutes of inactivity. By policy, vendor support personnel with administrative access to any hosted environment must configure their workstation environments to timeout and lock the screen after two minutes of inactivity.

10.6 Administrative Password Security

The Quest Managed Services and Solutions implementation meets the requirements as set out by the FDaaS RFP and the contract.

Quest Managed Services and Solutions does not reveal the exact password requirements but they meet the requirements of SSAE 16.

10.7 Media Destruction

This is handled as per the data destruction policy that ensures that the data is securely wiped and once this is completed, a data destruction certificate is issued to the customer.

10.8 Database Security

All access to the database is managed through two-factor authentication over an SSL VPN; each database administrator has unique access credentials to access all systems.

FDaaS-NV-DWSS database is stored on an encrypted file system and only authorized personnel and processes have access to the database.

10.9 Physical Security Controls

This requirement is met through the Quest Managed Services and Solutions certification of SSAE 16.

10.10 Other Security Controls

The FDaaS system employs a number of additional facilities for administrative personnel to review and enforce security restrictions. Extensive activity logging and real-time security monitoring and event notification are native features of the architecture.
11. Security Plan Approval

The undersigned acknowledge that they have reviewed the Pondera FDaaS Security Plan for NV-DWSS and agree with the information presented within this document. Changes to this Security Plan will be coordinated with, and approved by, the undersigned, or their designated representatives.

Signature: ___________________________ Date: ______________
Print Name: Robert Dehnhardt
Title: ISO
Organization: NV. Div. of Welfare and Supportive Services
Role: Information Security Officer

Signature: ___________________________ Date: ______________
Print Name: Donald Carter
Title: CSO
Organization: Pondera Solutions
Role: Chief Security Officer

Signature: ___________________________ Date: ______________
Print Name: Asif Ahmed
Title: CTO
Organization: Pondera Solutions
Role: Chief Technology Officer