Security Architecture Review (SAR)

1.1 Description of the Business Process

Provide a brief description of the business process as it is supported by the system:

https://www.maxpanda.com/helpmemax/

1.1.1 Operational Information

The Maxpanda SaaS solution is a multi-tenant ASP.Net application running in a US Based AWS region. Maxpanda leverages the AWS EC2 and RDS cores services with other supporting services.

Clients connect to https://app.maxpanda.com using SSL for all connections.

1.1.2 System Information

Maxpanda is a multi-tier ASP.Net application running on the Windows Server stack. The User interface is built using the Razor presentation framework from Microsoft with a MySQL database.

Amazon AWS Network tools are used with monitoring providing by the AWS Cloudwatch tools.

1.1.3 System Environment

Describe key aspects of the system operating environment beginning with the following key data points in Table SAR-1 and conclude with a detailed discussion of the essential security support structure of the system.

Table SAR-1. System Environment

System Environment	Response Data
Is the system owned or leased?	Maxpanda uses a combination of AWS IaaS components.
Is the system operated by the State or by a support service contractor?	Operated privately

System Environment	Response Data
If the system is maintained by support service contractor, describe comprehensively how the system is managed.	Operated privately, relying on IaaS from Amazon AWS
If the system is operated by the state-run consolidated data center, provide the name, location and point of contact for the consolidated data center.	We operate out a US based AWS region
Provide the hours of operation if this is a facility where the system is hosted: e.g., 24x7, M–F 7:30 am – 5:00 pm.	N/A
Document the approximate total number of user accounts and unique user types (i.e., researchers, programmers, administrative support, caseworkers, and public-facing employees).	Maxpanda separates non-prod and prod access. A limited number of prod accounts exist. Less than 5 admin accounts have access to the production environment.
Identify critical processing periods (e.g., eligibility processing).	N/A
If system serves a large number of off-site users, list both the organizations and types of users (e.g., other agencies).	N/A
Is FTI being processed or stored in this system?	I do not know what FTI is. Maxpanda is a Facility Maintenance tool. We store work order information about physical assets and locations. We do not store personal information.
List all applications supported by the system including the applications' functions and the information processed.	
Describe how system users access the system (i.e., desktop, thin client, etc.). Include any information required to evaluate the security of the access.	Access is supported through a web browser or an IOS/Android application.

Use Table SAR-1 to address the following items:

Provide a description of the system environment: If the system is maintained and/or operated by a contractor, describe (comprehensively) how the system is managed.

If the system serves a large number of off-site users, list both the organizations and types of users (e.g., other agencies, assistors, navigators).

Describe all applications supported by the system including the applications' functions and information processed.

Describe how system users access the system (i.e., desktop, thin client). Include any information required to evaluate the security of the access.

Describe the information / data stores within the system and security controls that limit access to the data.

Describe the purpose and capabilities of the information system. Describe the functional requirements of the information system. For instance:

- Are boundary protection mechanisms (i.e., firewalls) required?
- Are support components such as web servers and e-mail required?
- What types of access mechanisms (i.e., telecommuting, broadband communications) are required?
- Are "plug-in" methods (Mobile code; Active-X, JavaScript) required?
- What operating system standards, if any, are required?

Use Table SAR-2 to provide more details regarding system users including the following items:

User types

Organizations (internal and external) comprising the user community

Users' level of access (e.g., read-only, alter, and the like)

Uniform Resource Locator (URL) for web-based access

How the system is accessed

Table SAR-2. System Users

User Type (Group or Role)	Internal / External	Access Rights (Read, Write, Modify, Delete	Data Type Accessed	Expected Output / Product	User Interface (How system accessed – TCP/IP, Dial, SNA, etc.)	Web-Based Access (Provide URL)	Comments
Company Admin	Internal	Full rights	All Data		Browser	App.maxpanda.com	
Company Editor	Internal	Modify within company			Browser	App.maxpanda.com	
Site Admin	Internal	Create and modify wiithin Site	All data within assigned sites		Browser	App.maxpanda.com	
Site Editor	Internal	Modify within site	All data within		Browser	App.maxpanda.com	

			assigned sites				
Supervisor Unlimited	Internal	Create and modify within assigned areas	Buildings, Locations, WorkOrders		Browser	App.maxpanda.com	
Supervisor Limited	Internal	modify within assigned areas	Buildings, Locations, WorkOrders		Browser	App.maxpanda.com	
Staff Unlimited	Internal	Modify	Buildings, Locations, WorkOrders		Browser	App.maxpanda.com	
Staff Limited	Internal	Modify	Buildings, Locations, WorkOrders		Browser	App.maxpanda.com	
Submitter Unlimted	Internal	Read/Create	New WorkOrders		Browser	App.maxpanda.com	
Submitter Limited	Internal	Read/Create	New WorkOrders		Browser	App.maxpanda.com	
Tenant Unlimited	External	Read/Create	New WorkOrders		Browser	App.maxpanda.com	
Tenant Limited	External	Read/Create	New WorkOrders		Browser	App.maxpanda.com	
Viewer	Internal	Read Only	Work Orders		Browser	App.maxpanda.com	
Viewer Unlimited	Internal	Read Only	Work Orders		Browser	App.maxpanda.com	
Vendor Unlimited	External	Modify	Assigned WorkOrders		Browser	App.maxpanda.com	
Vendor Limited	External	Modify	Assigned WorkOrders		Browser	App.maxpanda.com	

1.1.4 Architecture and Topology

Maxpanda is a multi-tier web application. Access from the public uses https and SSL 1.2. All internal access between nodes uses the AWS VPC security controls in additional to encrypted SSL 1.2 traffic.

1.1.5 System Boundary

External traffic to Maxpanda is restricted to https over port 443. Once a user is authenticated, an encrypted authorization token is stored as a browser cookie. The ASP.Net security provider validates the encrypted token on each Get/Post action to the server.

1.1.6 Primary Platforms and Security Software

Maxpanda has selected Amazon AWS as our IaaS provider and therefor utilizes the tools and controls provided by AWS. Maxpanda uses the AWS VPC with Network ACLs and Security Groups to control access. Cloudwatch is used to monitor the infrastructure.

1.1.7 Interconnectivity Interfaces, Web Protocols, and Distributed and Collaborative Computing Environments

Maxpanda communicates between nodes using port 443 using SSL 1.2

1.1.8 Other Special Security Concerns

- N/A

1.2 System Interconnection / Information Sharing

Maxpanda does not directly connect to customer systems.

- Table SAR-3. Interconnections

Connecting Entity	System Name	Internal / External	Interconnection Type (How system accessed – TCP/IP, Dial, SNA, etc.)	Authorized Access Agreement in Place (ISA, MOU, BPA, etc.)	Name & Title of Authorizing Management Official(s) and Date of Authorization:	Comments

1.3 E-Authentication Assurance Level

Required to ensure that only authorized individuals have access to certain data classification resources. A critical step in this process is establishing confidence in a user's identity through adequate vetting and the provisioning of suitable authentication credentials.

NIST Special Publication (SP) 800-63-2, *Electronic Authentication Guidelines,* defines four (4) levels of assurance for electronic transactions. Table SAR-4 presents the Authentication Requirements by Assurance Levels.

Table SAR-4. Authentication Requirements by Assurance Levels

Authentication Assurance Level	Identity Proofing Requirements (See SP 800-63-2 for full requirements)	Authentication Requirements
Level 1 affords little or no confidence in the asserted identity's validity.	Identity proofing relies on the subscriber's own assertions.	Single factor authentication, such as a username and password, is adequate.
Level 2 provides some confidence in the asserted identity's validity.	Identity proofing requires verifying the individual's government-issued ID or financial account information, and other information.	Single factor authentication, such as a username and password, is adequate.
Level 3 provides high confidence in the asserted identity's validity.	Identity proofing requires verifying the individual's government-issued ID, a financial account information, and other information.	Multi-factor authentication is required.
Level 4 provides very high confidence in the asserted identity's validity.	In-person proofing is required.	Multi-factor authentication is required.

The OMB guidance, which is supplemented by NIST SP 800-63-2, provides agencies with criteria for determining the level of e-authentication assurance required for specific electronic transactions and systems based on the risks and their likelihood of occurrence (e.g., authentication errors and misuse of credentials).

Indicate the type of E-Authentication Assurance and authentication type used for each user role in the cell for Response Data in Table SAR-5.

Table SAR-5. E-Authentication Assurance Levels

User Role	Assurance Level	Authentication Type
All Maxpanda	Level	User name and password

1.4 Review of Security or Privacy Controls

This information is confidential to Maxpanda.