**BACKGROUND**

The Accounts Payable System (APS) is used to open Purchase Requests (PRs), manage Purchase Orders (POs), enter Invoices, and pay vendors.

APS is a vendor-supplied application provided by AP International. Widget World is operating on v7.4.

APS is installed on a UNIX server (APS\_Prod1) located in the Sacramento Data Center, and is administered by the APS Administrators in the San Francisco building. APS uses an Oracle 11g database.

**USER ADMINISTRATION**

**Access Path**

To gain access to APS, users must first log onto their workstation, which also logs them onto the network via Windows Active Directory. Once logged on, they open APS and enter their APS username and password.

**Adding New Users**

New users must complete an Access Request Form (ARF), which includes their name, title, and the access level(s) being requested. ARFs must be approved by the user’s manager and sent to the APS Administrator. The APS Administrator sets up the access, then emails the new account detail to the user. The email instructs the user to contact the APS administrator via phone, and the administrator will give the user the initial password over the phone. The user will be forced to change their password during their first login by the application. Once the process has been completed, the APS Administrator files the completed request forms in the Operations Center.

**Modifying Existing Users**

Existing users who need to modify their access in APS follow the same ARF process described above for new users. The only difference is that the APS administrator will also evaluate the need for the access levels previously requested and remove any access levels that are not needed for the user’s new job responsibilities.

**Removing Terminated Users**

Human Resources (HR) sends a list of terminated employees to all system administrators weekly. Upon receipt, the APS administrator will delete the user access for any employees with APS accounts. In the event of an ‘emergency termination,’ either HR or the user’s manager will notify IT immediately, who will terminate access immediately.

**Administrator Access**

There are four APS Administrators. When a new system administrator joins the team, the Lead Administrator adds their user account and related access levels. Since the administrator team is so small, they work in the same room and under the direct supervision of the Lead Administrator, which is appropriate. When an Administrator leaves the team, the Lead Administrator will immediately remove that Administrator’s Administrator account.

**User Access Reviews**

On a quarterly basis, the APS Administrator will create an access list of active APS accounts for each APS manager. APS Managers are asked to review the list to confirm that each employee is still employed within their department and that the access levels granted are appropriate for the users’ current job responsibilities. Any exceptions are noted on the report, and the APS Manager and APS Administrator work together to correct them. Once completed, the APS Manager signs and returns the reports to the APS Administrator, who files them in the Operations Center.

**Monitoring User Activity**

Widget World uses the Big Brother application to monitor all activity on its networks, applications, databases, and servers. Big Brother screens the logs from all those technologies and screens for patterns of suspicious activity. Any suspicious activity noted triggers an email and text message sent to the APS Administrators. The APS Admins investigate the alert, take the appropriate action, escalate as necessary, and ensure the matter is resolved timely. All of this activity is logged within the related ‘Trouble Ticket’ within Big Brother.

**Authentication**

APS uses passwords to authenticate users.

**Password Controls**

APS configurations require users to use strong passwords, as noted below:

* Minimum Password Length 8
* Maximum Password Length 12
* Construction – Passwords Must Contain:
  + At least one upper case and one lower case alphabetic character
  + At least one number
  + At least one special character
* Passwords may not be dictionary words
* Passwords may not be the same as the username
* Passwords may not contain more than two repeating characters
* Minimum password age 30 days
* Maximum password age 90 days
* Password history Users must change passwords eight times before reusing them

**CHANGE MANAGEMENT**

**Initiation**

Two types of changes can be made: (1) a bug fix, or (2) an enhancement. New change requests can be initiated by a Manager or above by calling the Help Desk. The Help Desk will open a Change Request ticket in the Y-Change application. The ticket identifies the requestor includes the reason for the change. If the change request is to fix an operations problem, it will assigned a ‘Severity 1’ rating and will be treated as an emergency change (see “Emergency Change” section below). All other changes are assigned a lower rating.

**Approval**

Change requests are reviewed by the Change Review Committee (CRC) in a weekly meeting. The committee decides if the request is for valid business reasons, considers the Return On Investment (ROI), approves the request (if appropriate), and assigns the request to a developer. Requests that are not approved are communicated to the requestor by the Help Desk, including the reason why, and the request ticket is closed.

**Development**

The developer makes the change in the Development Environment, which is a separate server than the production environment, and performs unit testing.

**Testing**

Once the change successfully passes unit testing, the developer moves the change to the Testing Environment, which is a separate server than the production environment. The developer will note the move in Y-Change, which notifies the Quality Assurance (QA) team that the change is ready for integrated testing.

The QA team performs integrated testing. Any bugs noted during testing are recorded in Y-Change, which will route the change back to the developer to fix. Once all the bugs have been fixed, the developer will route the change back to QA in Y-Change for retesting. Once all the bugs have been fixed and the change has successfully completed integrated testing, QA updates the status in Y-Change.

**User-Acceptance Testing**

Once the change has passed integrated testing, the requesting user is involved to perform User Acceptance Testing (UAT), to confirm that the change functions as requested and doesn’t have any other unintended consequences on the system.

**Final Approval**

All successfully tested changes are reviewed in the weekly CRC meeting. The test strategy and results are reviewed, along with the implementation strategy, contingency plan (in case the change doesn’t work in production), and the back-out plan. If everything is acceptable, the changes are approved to move to production. Approvals are noted in Y-Change.

**Move to Production**

Once the change has been approved by the CRC, it is scheduled to move into production. Users are given notification of any downtime, and the change is moved in during the scheduled change window. The operator implementing the change does not have any development or testing duties, and is therefore segregated from those portions of the process. Once the change has been successfully implemented, an email is sent to the users to notify them of the change, and the Change Request is closed.

**Emergency Changes**

Emergency changes are usually when a crucial system is down, which requires immediate attention to bring it back up as soon as possible. In those situations, all emphasis is placed on recovering the affected system(s). The change management process, described above, is generally followed during these situations. However, there is close supervision of all recovery activities by the Operations Manager on duty. After the system(s) have been recovered, all documentation is created afterwards, and an incident report is created and discussed in the next CRC meeting.

**IT OPERATIONS**

**Physical Security**

The data center is located within the Sacramento facility. Electronic card-keys are required to enter the building and are required again to enter the data center within the building.

Only authorized employees are allowed into the building. Anyone else (e.g., contractors, visitors, etc.) must sign-in with Security at the front desk. They enter their information into the appropriate log, and Security assigns them a temporary visitors badge. All visitors must be escorted at all times. Visitor badges are designed to turn red after 24 hours, so the badges cannot be reused.

Only Administrators, Building Security, and Maintenance personnel are allowed into the data center.

Security guards are onsite 24 hours a day by seven days a week. There is one at the front desk and another that walks the facility once an hour.

Video surveillance cameras are located at all points of ingress and egress to the building and the data center. Other cameras are also located in strategic locations. All video surveillance is monitored by the security guards at the front desk. Video is maintained for 30 days on the video surveillance system’s hard drive.

Badges must be worn and visible at all times, including both employees and visitors. Employees are encouraged to challenge anyone in the building without a badge and notify security if they don’t have one.

**Physical Safeguards**

The data center is equipped with the following physical safeguards:

* Raised floors
* Leak detection system
* FM200 Fire suppression system
* Four Type C fire extinguishers located throughout the raised floor area
* Very Early Smoke Detection Apparatus (VESDA) System
* Air conditioning units within the data center, in addition to the building’s air conditioning
* Power conditioning and distribution units
* Universal Power Supply (UPS) equipment sufficient to run the data center for 90 minutes in the event of a power outage
* A backup generator with enough fuel to run the data center for seven days
* Emergency power-off switches located at each door to the data center

The leak detection, VESDA, and fire detection & suppression systems are linked to control panels located in the operations center and the front desk, so they can be monitored by the system administrators and building security.

**Scheduling**

Scheduling requests follow the change management process outlined above. Most scheduling requests are for interfaces, backups, or regular reports.

**Monitoring**

The Operations team monitors the status of all scheduled jobs for failures using the iMon monitoring tool. iMon also monitors server and database availability. All failures trigger automatic alerts that are displayed on the iMon control screen, which runs on each Operation Team member’s workstation as well as a giant screen mounted on the front wall of the Operations Center. iMon will also open a trouble ticket automatically in FixEm, the Hel p Desk application.

**Problem & Incident Management**

The Operations Team receives alerts from both Big Brother and iMon (see User Administration – Monitoring and Operations – Monitoring sections above). Both systems have interfaces into FixEm, the Help Desk application. In addition, the Help Desk team receives phone calls and emails regarding matters that also initiate manually-entered FixEm tickets.

All trouble tickets are assigned a severity ranking. Severity 1 tickets are the most urgent, and must be addressed immediately. Severity 2 tickets are required to be resolved within 24 hours. Severity 3 tickets are required to be resolved within seven days. Any tickets that are not resolved within the required timeframe for its severity will automatically be escalated up the Severity rankings at the end of its resolution window. All tickets are discussed daily in the 8 AM Operations Team Meetings to allow for collaboration, escalation, and the timely resolution of incidents.

**Backups & Recovery**

All servers are backed-up on a regular basis, according to the following schedule:

* Full system backups monthly
* Full data backups weekly
* Incremental backups daily

Backups are written to tapes, which are rotated offsite on a weekly basis using the Steel Cave document storage service. Steel Cave provides containers to Widget World, which the company can lock with its own padlocks. Tapes are packed into the containers, a Steel Cave transmittal notice is completed using the Truckin application provided by Steel Cave, inventorying the tapes located in that container. Hardcopies are printed to accompany the container.

When Steel Cave picks up that container, the Transmittal Notice is signed by both the Steel Cave representative and the Operations Team member on duty that day. Steel Cave also delivers a container at the same time. Another Transmittal notice accompanies the return, which is also signed by both parties. Both outgoing and incoming transmittal notices are filed in the Operations Center.

**Business Continuity Planning (BCP)**

Widget World has a Business Continuity Plan (BCP), which includes the following sections:

* Risk Analysis
* Business Impact Analysis
* Executive Crisis Communication & Coordination Plan, Including Contact Lists
* Recovery Strategy for All Critical Systems
* Manual Processes For All Critical Functions During The Disaster Event, Including Manual Controls Necessary To Accomplish All Objectives Of Critical Functions
* Post System Recovery Strategy (Getting The Manual Transaction Data Into The Recovered Systems), Including Controls
* Media & Government Officials Liaison Policies & Procedures
* Document Testing Requirements & Schedule
* Document Maintenance Requirements & Schedule

**AntiVirus / AntiSpyware / Etc.**

Bug-B-Gone software is installed on all critical servers and workstations. It is configured to automatically update its virus and other definitions on a daily basis. If viruses or other malicious software is detected, an alert is sent to the Operations Team and the normal Problem & Incident Response activities (described above) are followed.