Westaff®

Information Technology Policies and Procedures

Version 1.2 Release: February, 2009

Revision Date: 2/9/09

Table of Contents

Introduction

Information management is a crucial component in modern business. Creating, managing, and caring for the computer and network systems on which Westaff's information resides is the responsibility of Westaff's Information Technology department. To better fulfill the duties and responsibilities inherent in that responsibility, the department has created these policies and procedures.

Overview

The policies and procedures are grouped as shown below.

Group	**Policies and Procedures for**
Access Controls	Creating, changing, removing, and reviewing the accounts and software used to gain electronic access to Westaff's information systems.
Authentication	Launching applications which are used to create and modify information that is used in Westaff's financial reports.
Backups	Creating and managing the data backups which would be used to restore Production data in the event that the data in the Production environment became destroyed or corrupted and was no longer of any use.
Change Control – Application	Making software operating system changes to the applications used within Westaff's Production and Test environments.
Change Control – Patches	Making software operating system changes to the servers and databases within Westaff's Production environment.
Password Controls	Creating, changing, and removing the passwords which are used with login names to safeguard Westaff's information systems.
Physical Safeguards	Creating, removing, and reviewing the lists which are used to determine who can access the physical locations which house Westaff's information systems.
Restores	Recreating the Production environment in the event that the environment is lost or is no longer able to be used.
Segregation of Duties	Reviewing access within 2nd Wave and PeopleSoft provided to individuals to carry out their assigned work responsibilities.

Within each group, the policies that govern the subject of that group are subdivided by area of focus. In a separate group after the policies are the procedures also subdivided by area of focus. The procedures give the step-by-step instructions used to implement the policies.

At the end of the document are several appendices which provide additional information. This information is expected to change more frequently than the policies and procedures specified in the main document so each appendix has its own change log.

Policy and Procedure Review

Once a year the IT management team reviews this document and proposes changes to update the document. The QA Manager or designee incorporates the changes and provides the updated document to the Chief Information Officer for his or her review and approval. Each appendix is reviewed annually with this document. If the information in an appendix is changed between review periods, the date and approval of the changes contained in the appendix are noted on the appendix itself.

Approval

Author	Date	Approved By	Date Approved
______________________	________________	______________________	________________
Jim Driggers, QA Manager		Andy Elgazzar, VP of IS	

Change History

Date	By	Action	Section
10/29/08	Jim Driggers	Updated	PS and 2nd Wave Access Review procedures Creating, Changing, Removing Domain Accounts procedures Reviewing Domain Accounts, Disaster Recovery
2/6/09	Jim Driggers	Updated	Added “or designee” to all titles, replaced CIO references with “VP of IS”, changed Firewall and VPN Connectivity reviewer, updated procedures for Creating, Changing, Removing Domain Accounts, updated procedure for reviewing PeopleSoft and 2nd Wave access, removed review of Ready_Key access log from Physical Safeguards procedures, clarified authority to migrate emergency changes to production prior to getting approval, added testing requirements for Major Project changes.

Access Controls

This section provides the policies and procedures to be used to safeguard access to Westaff's computer systems and the data on those systems.

Policies

Network and Application Access

User access to Westaff's information systems is governed by the use of user domain accounts and security groups within Active Directory (AD). The domain account is added to security groups, which enables access to the application and folder whose access is controlled by that security group.

- Access to 2nd Wave is controlled by the user's domain account and group membership allowing access to the 2nd Wave executable. An additional 2nd Wave specific user account profile is established within the 2nd Wave application allowing the domain account to sync with the user profile. 2nd Wave permissions are controlled within the 2nd Wave user profile which is separate from the user's domain account.
- Access to PeopleSoft is created by adding the corresponding role to AD. With the exception of generic domain accounts, all users accessing PeopleSoft Financial Management System (FMS) and Human Capital Management (HCM) use Lightweight Directory Access Protocol (LDAP). **PeopleSoft Staffing Front Office (SFO) does not have LDAP active. Therefore PeopleSoft security for SFO is handled in PeopleSoft.**
- Access to End User Computing (EUC) "critical documents" is created by adding the user's account to the security list of the folder containing the applicable EUCs. A select number of critical financial documents have been identified and are kept within folders that are managed by the associated business owners. Only select individuals have access to each of these documents on an individual basis. Additionally, only the owner of the document may request and grant additional access to the associated document. Requests will be placed through the Support Center and documented in Remedy. The folder structure and owners are outlined in Appendix H: EUC Folder Structure.

A request is placed with the Support Center to grant, modify, or remove access to Westaff's information systems, including 2nd Wave, PeopleSoft, and folders containing EUC files. New accounts and account terminations are handled through the PAF (Personnel Action Form).

A PAF should be submitted at least three business days prior to the person's first day of employment. For terminations, the PAF should be submitted by the manager, which is then delivered to Human Resources and the IT Support Center, prior to the employee's last day of employment.

A Remedy change request is used to document changes to domain accounts. This includes creation, modification, and deletion of domain accounts. Approval from the user's manager will be included in the Remedy ticket. The approval will be evidenced either by the PAF being sent by the manager or by a separate e-mail from the manager authorizing the change.

Domain Account Review Procedures

Periodically a review will be made to ensure system access granted to domain accounts. These reviews will be recorded in Remedy as a Change Ticket using the Category Type Item (CTI) hierarchy below:

- Category = Account
- Type = SOX
- Item = Account Review

In the audits below, the IT reviewer should mark "OK" by those names that are approved and line out those names that should be deleted. A separate Remedy change request ticket should be created for each account to be deleted. These separate tickets should follow the standard procedures used by Support Services for account changes.

Inactive Domain Account Review: Support Services will perform a quarterly (every 90 days) audit of domain accounts to ensure all unathorized accounts have been disabled or deleted. Domain accounts are managed using AD. Unauthorized domain accounts are defined as domain accounts related to terminated employees, employees on long term leave or a domain account that has not been used to log into Westaff's network within 90 days.

Developer/DBA Access Review: To maintain a secure environment and ensure that code is not altered in Production environments by bypassing Westaff's change control process, the Director of Enterprise Information Systems (EIS) will perform a semi-annual audit. The audit will consist of reviewing access to Production and Test systems to ensure the following:

- Developers and technical consultants do not have access to change code directly in Production or Test environments
- Only authorized database administrators have access to make changes in the Production and Test environments

The following systems are in scope for this analysis: 2nd Wave, PeopleSoft Entreprise Solution (SFO, HCM, FMS.)

The IT Manager or designee will be reponsible for auditing operating system level access. If the Director of EIS or IT Manager are unable to complete the review, the designees are responsible to complete the review.

End User Computing File Access Review: To prevent unauthorized file modification, the owner or designee of the folder containing the EUC files will perform a semi-annual audit. The IT Manager or designee will provide a listing of those domain accounts that have access to the folder.

PeopleSoft and 2nd Wave Access Review: The IT Department generates a listing of all current Westaff employees and of affiliates authorized to access 2nd Wave. For each person on the listing, their roles in PeopleSoft HCM and FMS, the offices in 2nd Wave to which they have access, and in which office(s) the person has payroll access and/or Send Data access is listed.The IT Department will generate the list semi-annually. The list will be sent to each Reviewer as identified in Appendix I: Periodic Review Schedule for review by them and their designees. Reviewers or their designees will review the accounts and permissions on the list using the Segregation of Duties matrix, note any changes that need to be made, and return the lists to Support Services. Any changes to be made will be requested via submission of email or a PAF if a termination, title change or new account is involved. Support Services will create a Remedy change request to document the review. The Chief Operations Officer (COO), Chief Financial Officer (CFO), Vice President of Information Services (VP of IS), Vice President of Field Operations, and Vice President of Franchise Operations or authorized designees are responsible for ensuring their employees complete the review. The Vice President of Field Operations will be assisted by the Director of Field Support or other authorized designees to ensure review of Westaff field office user accounts is completed.

Operating System Access Review: Only IT Engineers and DBAs have direct access to operating systems on servers. When an IT Engineer or DBA's employment is terminated and no further contact is expected with the employee (for example, the terminated employee will not be hired back as a contractor), the IT Manager or designee will have that account removed from the servers and have the server administration passwords changed to prevent unauthorized access. Server access will be reviewed per Appendix I: Periodic Review Schedule.

Database Access Review: Only DBAs and system accounts have direct write access to PeopleSoft databases in Production. When a DBA's employment is terminated and no further contact is expected with the employee (for example, the terminated employee will not be hired back as a contractor), the Director of EIS will have that account removed from the servers and have the database passwords changed to prevent unauthorized access. Database access will be reviewed per Appendix I: Periodic Review Schedule.

Firewall

Westaff's Firewall is protected by a Cisco PIX Firewall.

The configuration of the Firewall will remain as secure as possible and will only be changed if a valid business need should require it. Ports and access lists will remain as restricted as possible and all changes will be analyzed by the Network Engineer to ensure all risks are mitigated prior to making any changes.

Any changes to the Firewall must be approved by the VP of IS or designee.

Wireless Connectivity

Requests to have wireless connectivity must be approved by the Network Engineer or by the IT Manager or designee. All requests will be approved as long as the following requirements are met:

- Up-to-date virus definition
- Built-in 802.11x wireless card is present
- Laptop is Westaff owned or if personal computer then manager has approved its use
- Requester is a Westaff FTE corporate employee

VPN Connectivity

The VPN client will be issued as a last resort means of remote access and only if the user requires access to services that cannot be delivered by the Portal of other non-VPN connection methods.

Requests to have VPN access must be approved by the requester's manager and the Network Engineer or designee.

Procedures

Creating, Changing, Removing Domain Accounts

When a person is hired by Westaff or a Westaff Affiliate and that person requires access to the applications and data provided through Westaff's computer network, an account is created for that person. The PAF, located in the Forms section of Outlook, is used to request the creation of an domain account for the person.

In the PAF, the requesting "Manager" identifies the requested action (New hire, termination, promotion etc.) and completes the other information required by Human Resources. Once fully completed and submitted, the form is automatically sent to the Support Center distribution list. Once received, a Remedy ticket is created and the PAF is copied into it. Permissions and Segregation Of Duties (SOD) will be determined by what was requested on the PAF along with the controlling Permissions Matrix document. Requested changes that create a SOD conflict will be escalated to the Westaff Internal Auditor for review and direction.

If the PAF did not originate with the manager of the user whose access is being set up, modified, or deleted, then Support Services will obtain written approval from the user's manager before implementing the requested change.

If the person is a Westaff employee, Human Resources reviews the PAF and then gives approval to Support Services. Support Services may begin setting up the account before getting HR approval, but will not implement the requested change until HR approval is received.

If the person is an Affiliate employee, the approving manager fills out the PAF and submits it directly to Support Services. Upon receipt, Support Services verifies the approving manager and creates the account.

In both cases, a Remedy ticket is created to document the actions taken by Support Services to set up and implement the requested domain account changes. The actions above will be recorded in a Remedy change request using the CTI below:

- Category = Account
- Type = Field or Corporate as appropriate
- Item = New User for creating a new user, or
- Item = Delete for deleting a user, or
- Item = Modify Access for changing a users' access

Title/department/role changes will result in permission changes based on the Permission Matrix document. Screen captures will be taken as specified below and recorded in the Remedy ticket.

For new hires Support Services will take the following screen captures:

- A screen capture of the profile is being used to base the new hire's security access
- A screen capture of the new hire's security access, after the new hire's security has been set up

For changes that involve security access changes, the requesting manager must listed the required access and e-mail approval for the access change. Support Services will take the following screen captures:

- A screen capture of the profile is being used to base the person's new security access, if the new security is based on another person's access
- A screen capture showing the person's security access before changes are made
- A screen capture showing the person's security access after the changes have been made

Approved termination requests will result in that account's password being changed thus locking the terminated employee out of Westaff's network. Unless otherwise instructed and if Support Services receives notification before 5:00 PM Pacific Time, the password will be changed at the later of the following:

- At a time equivalent to the end of the user's last employed business day in the user's time zone
- Within four hours of Support Services receiving the notification

For terminations requiring more timely action, Support Services will change the password immediately following notification from the terminating manager. For terminations for cause, the password change will be handled as an Urgent request.

After the password has been changed, if the terminated user had access to PeopleSoft, the person's login name will be locked. A new password will be offered to the Manager for a period of 10 days for review. Following the review period, and once Support Services receives the Manager's approval, the following actions will be taken:

- Delete the user's domain account. Doing this will prevent access to the network and to all folders containing EUC documents. This will also remove the user's access to 2nd Wave, since 2nd Wave requires a directory in which to write debug log entries for each user.

Passwords for generic ids will be changed upon termination of any employee with knowledge of the password. All such changes will be documented in a Remedy change request ticket using the CTI shown below:

- Category = Account
- Type = Corporate
- Item = User Security

An exception to this policy is made if the employee is expected to need access to Westaff's network. If this is the case, the employee's domain account will be disabled and moved to the vendor Organizational Unit (OU). Changing the person's account in this way will be recorded in Remedy.

Reviewing Domain Accounts

Inactive Account Review: Javelina is scheduled to produce an AD report at least every 90 days. This report contains domain accounts with 90 days of inactivity and is sent directly to Support Services. Support Services opens a new Remedy ticket and documents the following within the ticket:

- The report outcome
- Steps taken to validate the domain accounts

The user's Manager is contacted and written validation of decision is required before the account is terminated. If the domain account is to be terminated, a PAF will be required from either the Manager or HR and the steps taken, including the specific domain accounts that have been disabled or deleted will be documented in Remedy.

The ticket will contain the reasoning behind retaining domain accounts that reside on this report. Domain accounts that should be terminated on this report will require a PAF and Support Services will send HR an e-mail requesting a supporting PAF if one wasn't received. System, vendor, and test domain accounts will not require a PAF for deletion.

Operating System Review: An AD report will be generated semi-annually. This report contains a list of accounts that have access to server Operating Systems. The IT Manager or designee will generate this report using Hyena. The IT Manager or designee evaluates the report to ensure there are no unauthorized accounts having undue access. The IT Manager or designee updates the Remedy ticket with the following information:

- Audit results
- Action taken

Developer/DBA Access Review: An AD report will be produced semi-annually. This report contains a list of existing domain accounts and roles associated to these domain accounts. This report is sent to Support Services. Support Services opens a new Remedy ticket and assigns this ticket to the Director of EIS. The Director of EIS evaluates the report to ensure that developers and technical consultants do not have access to change code online in PeopleSoft and updates the ticket with the following information:

- Audit results
- Action requested

Additionally, the Director of EIS will generate a list of users/access methodology. All FMS and HCM users should have access through LDAP only.

For PeopleSoft SFO, the Director of EIS will generate a list of user and roles associated to these domain accounts. The Director of EIS evaluates the report to ensure that developers and technical consultants do not have access to change code online in PeopleSoft

End User Computing File Access Review: A report will be produced semi-annually. The report lists which domain accounts have access to the folders containing the files listed in Appendix C: EUC File Review. A Support Services Specialist opens a new Remedy ticket using the CTI shown below and assigns this ticket to him or herself. Support Services subdivides the report by folder and sends an e-mail review request to the owner of each folder. The request will be for the owner to evaluate the report and note the following information on the report:

- Whether the domain account should have access to the listed folder(s)
- Whether the domain account's access should be removed from the listed folder(s)

The report is returned to Support Services who attaches the report to the Remedy ticket. If changes are needed, the business owner will outline these changes in an email to Support Services. These reviews will be recorded in Remedy as a Change Ticket using the Category Type Item (CTI) hierarchy below:

- Category = Network
- Type = Corporate Support
- Item = Drive Permissions

PeopleSoft and 2nd Wave Access Review: The IT Department generates an AD listing of all current Westaff employees and of affiliates authorized to access 2nd Wave and/or PeopleSoft. For each person on the listing the following is listed:

- Their roles in each PeopleSoft database (SFO/HCM/FMS)
- The offices in 2nd Wave to which they have access
- In which office(s) the person has payroll access
- In which office(s) the person has Send Data access.

This listing is sent to Support Services. A Support Services Specialist opens a new Remedy ticket using the CTI shown below and assigns this ticket to him or herself. The specialist sends the listing to each manager listed in Appendix I: Periodic Review Schedule.

- Category = Account

- Type = SOX
- Item = Account Review

Each reviewer either reviews the listing or passes it down to one of their managers to review in order to ensure their employees have the correct access.

Where the listing indicates the employee has too much access, the reviewing manager updates the review(s) to indicate which access should be removed and returns the review to Support Center.

Support Center reviews the returned listings for completeness. If incomplete, Support Services contacts the manager and requests any missing information. For field office user reviews not turned in within a reasonable amount of time, the Support Service Specialist contacts either the Director of Field Support (for Westaff employees) or Vice President of Franchise Operations (for Affilate employees) to notify them of missing reviews.

The Director of Field Support and/or Vice President of Franchise Operations have ownership of getting the completed review returned to Support Services.

After reviewing the returned listings and attaching them to Remedy tickets , the returned reviews are sent to ISG to review to ensure the requested actions seem right. If no change is needed, ISG closes the Remedy ticket. If changes are needed, ISG either assigns the ticket to Support Center to implement or works with the reviewing manager to implement the requested access deletion.

Once the requested access deletion has occurred, the Remedy ticket is closed.

If the employee should have additional access, the reviewing manager completes a PAF to request the additional access using the normal procedures.

Firewall

Requests to change Firewall settings are be routed through the Support Center either by e-mail or via a phone request and a Remedy ticket is created to track the project.

A copy of the baseline Firewall configuration will be kept in a Remedy ticket and used to compare configuration changes as they are requested. Each change request requires review by the Network Engineer and is documented in a Remedy ticket.

The Remedy ticket is assigned to the Network Engineer. Once the Network Engineer determines that the requests are acceptable, approval is requested from the Business Manager or designee and VP of IS or designee.

The VP of IS or designee will annually compare the current Firewall configuration to the baseline configuration from the previous year. Any differences will be researched to ensure one or more Remedy tickets explain the variance.

Wireless Connectivity

Users may request wireless access through the Westaff Support Center. Wireless access is issued upon request providing the user has a Westaff issued laptop with an 802.11x wireless adapter. The Wi-Fi network is configured using WPA Enterprise AES encryption. Additionally users are required to authenticate with their AD domain account using Protected Extensible Authentication Protocol (PEAP)/Temporal Key Integrity Protocol (TKIP).

Westaff VPN Connectivity

Users may request remote access through the Westaff Support Center and will require the requester’s manager approval. The VPN is configured using 3DES/AES encryption with shared secret authentication. Additionally users are required to authenticate using their AD domain account. The shared secret password is changed and redistributed once per calendar quarter or upon a significant staff change. When the password is changed a Remedy ticket will be created to note the change (not including the specific password) and closed for documentation purposes.

Password Controls

This section provides the policies and procedures to be used in creating, controlling, and using passwords to access to Westaff’s computer systems and the data on those systems.

Passwords are an important aspect of computer security. They are the front line of protection for user domain accounts. A poorly chosen password may result in the compromise of Westaff's entire corporate network. As such, all Westaff employees (including contractors and vendors with access to Westaff systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Policies

Domain accounts consist of a login name and password. The login name is constructed by taking the initial letter of the user’s first name and combining it with the user’s last name wherever possible. The initial password is created by Support Services when the domain account is first created and the user is required to change the password upon first accessing Westaff’s network.

For PeopleSoft SFO, non-LDAP accounts are used if the person needs direct access to SFO. The non-LDAP account is created by a DBA within SFO using PeopleSoft security. The SFO login account matches the LDAP domain account of the person assigned to that SFO login account. The password for the non-LDAP account is created by the DBA when the account is set up and may or may not be changed by the user when the user logs into SFO. If the user logs into SFO via a link in either HCM or FMS, PeopleSoft ignores the password set in SFO and accepts the LDAP password using single-sign on functionality. If the user logs directly into SFO, then the user is required to enter the password as it exists in SFO.

The password policy requires:

- At least six alphanumeric characters long
- Can not use the 10 previously used passwords

The domain account password automatically expires after 90 days. When a password expires, a new password must be created by the user before AD will enable the user to access the network.

If an incorrect password is given more than 10 times in a row, AD will lock the user out of the network. If that happens, the user must contact Support Services to have the domain account unlocked. Support Services is able to change the password if the user requires it.

The PeopleSoft security system settings in Staffing Front Office exactly match the AD settings used to govern domain account password restrictions.

For any vendor-delivered generic id at the OS or Database level, its password will be changed upon software installation.

Passwords for generic ids will be changed upon termination of any employee with knowledge of the password. All such changes will be documented in a Remedy change request ticket using the CTI shown below:

- Category = Account
- Type = Corporate
- Item = User Security

An exception to this policy is made if the employee is expected to need access to Westaff's network. If this is the case, the employee's domain account will be disabled and moved to the vendor Organizational Unit (OU).

Passwords must not be inserted into email messages or other forms of electronic communication.

Westaff passwords should not be shared with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Westaff information.

If someone demands a password, the person should be referred to this document or instructed to contact Support Services.

If a domain account or password is suspected to have been compromised, the incident should be reported to Support Center. In such a case, the domain account or password should be changed to prevent possible unauthorized access.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Procedures

When Support Services receives a request to create a domain account from HR, a password is created in AD to go with that domain account. The password is set to require the user to change the password after the initial login.

If the user is authorized 2nd Wave access, Support Services uses the Security Tool to assign the designated offices to the user's login and provide Payroll, Send Data, and 2nd Wave report access per the PAF. Support Services will also create a shell domain account in PeopleSoft SFO, HCM, and FMS to enable 2nd Wave records created or modified by the user to be accepted in PeopleSoft. No PeopleSoft roles, permission lists or passwords are assigned in the shell domain account.

If the user is authorized PeopleSoft access, Support Services assigns the user's role based on a similar person's permissions in LDAP. The PAF specifies which person to base the new person's domain account.

If the user is to have a non-standard set of permission list(s) and/or page(s) within PeopleSoft, Support Services creates a Remedy change request using the CTI shown below and assigns the request to the Security group. The Security group sets up the authorized non-standard access in LDAP.

- Category = PeopleSoft
- Type = Request
- Item = Access

If the user needs a user account created in PeopleSoft SFO, Support Services creates a Remedy ticket using the CTI shown below and assigns the ticket to the Security group, which the DBAs compose.

- Category = PeopleSoft
- Type = Request
- Item = Access

The DBA creates an account or modifies the existing account as needed in PeopleSoft SFO using the same account name as the user is assigned in LDAP and adds the requested role(s). The DBA creates a password for the user and via telephone notifies the user what password to use for the non-LDAP account. With the exception of requiring a password change upon first login, non-LDAP account passwords in SFO are configured exactly as passwords in AD, e.g. expiring after 90 days, etc.

Authentication

This section provides the policies and procedures to be used to control access to specified systems after users have successfully logged into Westaff's computer systems.

Policies

Each person authorized to access Westaff's network is assigned a unique domain account. The domain account is used by LDAP to control access to Westaff's network, applications, databases (through the application), and folders containing EUC files. The domain account consists of a login name, usually consisting of the initial letter in the employee's first name and the employee's last name, and a password.

Generic IDs have been created for administrative purposes and are listed in Appendix G.

Metaframe Secure Access Manager (MSAM) is a terminal services application used by Westaff to enable its field employees to access their applications and data. All Westaff field users gain access to their applications through MSAM.

Both field and corporate users log into 2nd Wave using MSAM.

Field users access PeopleSoft directly to enter their own time. Time for temporaries is entered in 2nd Wave by field users and 2nd Wave passes that information to PeopleSoft through an interface. Field users do not enter time for temporaries directly in PeopleSoft.

PeopleSoft is Westaff's back office system and holds the company's financial and human resource data. Other than for certain HCM pages related to Employee Self Service (ESS) and Manager Self Service (MSS), only corporate users directly access PeopleSoft. ESS is mostly used by Westaff regular employees to enter their time worked and MSS is mostly used by managers to approve their regular employees' entered time worked.

Application Session Termination Policies

When a field user accesses applications through Westaff's computer system, the network creates an application session for that user. If there is no activity on that session for 105 minutes, the session is terminated. When a corporate user accesses any of the three PeopleSoft databases (SFO, HCM, or FMS) directly, PeopleSoft creates an application session for that user. If there is no activity on that session for 30 minutes, the session is terminated.

Procedures

Once the domain account has been created, adding the domain account to security groups is used to provide access to the applications, files, and resources governed by each security group. In this way, access is controlled to Westaff's computer network, 2nd Wave, and PeopleSoft.

Before gaining access to the network, the login name and password are authenticated against AD and LDAP. If a match is found, the user is permitted access. If the user logs into the system through MSAM, the system populates the MSAM desktop with the application icons listed in the user's profile.

To access 2nd Wave, users click on the 2nd Wave icon in the MSAM desktop. As part of the 2nd Wave login process, 2nd Wave verifies the user has access to at least one office within the 2nd Wave database and the user has a network folder in which 2nd Wave can write debug log entries. If the user does not have access, the login fails and an error message is written to the user's 2nd Wave debug log indicating the nature of the error. In each session, the first time the user clicks 2nd Wave's Timecard and Send Data buttons, 2nd Wave checks its security tables to determine if the user has been authorized those functions. If the user is not authorized those functions, an error message appears informing the user that the functionality is not authorized.

To access PeopleSoft, users launch a web browser and connect to the applicable PeopleSoft login web page. Each PeopleSoft database (SFO, HCM, and FMS) in each environment (Production, Development, Upgrade, Conversion, Beta, Alpha. Training, Education, and Demo) has its own login web page. The security in each database and environment is maintained within that environment. For Production, the security is maintained through a Westaff customization that uses LDAP, with the exception of SFO application. The first time a user launches a Production PeopleSoft database, a check is made against that user's LDAP settings and PeopleSoft creates a PeopleSoft account with the LDAP supplied settings for the user.

When accessing SFO in Production, whether by logging into SFO directly or by opening a page within SFO from a link in either HCM or FMS, PeopleSoft security within SFO checks the user's login name to determine whether the user's SFO account has permission to the requested page.

To access a folder containing EUC files, LDAP is checked to verify the user has been given authorization to open and edit those files. For EUC folders, access is provided at the individual domain account level rather than use membership in a security group. Users who have not been given access cannot access the folder or its contents.

Application Session Termination Procedures

When the user logs into MSAM the network creates a network session for the user. If there is no activity on that session for 90 minutes, the user's network session is terminated. For an additional 15 minutes, the application servers maintain an application session for that user internally. This means that if the user logs back into the system within 15 minutes of the system terminating the user's network session, the user will reconnect to the application session at the point at which they left it. If there is no activity on the application session for a total of 105 minutes, the application server will close the user’s application session. If this happens then all of the user’s unsaved work is lost and the user will have to launch each desired application manually.

Corporate users log into PeopleSoft directly through a web page accessed with Microsoft Internet Explorer. As part of the login process, PeopleSoft creates a session for the user. To better protect the information held within the PeopleSoft system, management has decided to only allow 30 minutes of inactivity on a PeopleSoft session before PeopleSoft will terminate the session. If this happens then all of the user’s unsaved work will be lost and the user will have to launch PeopleSoft manually. This 30 minutes of inactivity limit applies to all users regardless of whether PeopleSoft created the user’s account based on LDAP settings or the user’s account was manually created within PeopleSoft SFO.

Physical Safeguards

This section provides the policies and procedures to be used to restrict and review physical access to Westaff’s two data centers.

Westaff has contracted with Verizon Business to co-locate its primary data center facility (called Data Center 1 or DC1) in Sacramento. Westaff itself provides physical security and infrastructure at a secondary data center (called Data Center 2 or DC2) in its corporate headquarters location.

Policies

Access to the data centers is reviewed quarterly.

Access reviews is logged into Remedy using the CTI below:

- Category = Facilities
- Type = Westaff Support
- Item = Access Control

Access to the data centers is granted by the VP of IS or designee.

Procedures

Physical security to DC1 is maintained by Verizon Business. A list of authorized personnel has been provided to Verizon Business. When someone wants to physically enter DC1, Verizon requires people to identify themselves, fill out a sign-in log and deposit their driver’s license at the Security desk. Verizon checks to see whether the person is on the list of authorized personnel before allowing access to the facility. If the person is not on the list, Verizon contacts the IT Director of Operations or his/her designee to get authorization before allowing access to the data center.

Each quarter the VP of IS or designee will ask Verizon for a list of people authorized access to the data center. Once Verizon provides the list, the director handwrites “OK” beside each name that is valid, notes which names should be removed, scans the document, and attaches the softcopy to the Remedy ticket. For those names that should be removed, he sends an e-mail to Verizon asking them to remove access. Once he gets notification that they have removed access for the desired individuals, he attaches that notification in Remedy as well.

Physical security to DC2 is maintained through the use of a Ready-Key badge reader. Ready-Key is an electronic FOB configured to allow access to the corporate facilities. Access is defined on a per user basis and can be restricted by door, time, etc. The DC2 access list is approved by the VP of IS or designee. Access activity is recorded in the Ready-Key systems.

Change Control – Patches

This section provides the policies and procedures to use when introducing new software patches and upgrades to Westaff's Production and Test computer system environments.

Policies

Prior to requesting a patch be applied in the Production environment, the patch must be applied and tested in a non-Production environment.

Prior to applying each patch in the Production environment, the patch must be discussed and its application approved during the weekly Migration Review meeting.

Procedures

Once all testing is completed and the IT Engineer is ready to request approval and schedule maintenance or downtime to implement the change, a "Scheduled Maintenance Request Form" must be filled out and submitted. This form is located within Outlook in Tools/Forms/Choose Form/Organizational Forms Library and is called "Maintenance Notification".

The IT Engineer provides the required information, including an outline of the tests performed, known risks, contacts, etc. within the form.

Once submitted, the form goes to the Support Center, who creates a Remedy ticket and attaches the Maintenance Notification form to the ticket. The Remedy ticket is assigned to the QA Manager or designee, so the request can be discussed in the next weekly Migration Review meeting.

After the meeting, the QA Manager or designee sends an e-mail listing IT management's verbally approved changes to the VP of IS or designee and courtesy copies the rest of the IT managers. After the VP of IS or designee has replied with written approval, a maintenance notification is prepared and sent to Support Services. Support Services then issues an email message announcing the upcoming changes—whether or not any outage of service is expected. The communication should be published with a minimum of two business days advance notice.

The VP of IS or designee's approval e-mail will be embedded in the Remedy ticket's Activity Log.

The patch will be applied at times deemed appropriate by IT management.

Change Control – Applications

This section provides the policies and procedures to use when introducing software application changes to Westaff's Production and Test computer system environments. The following software systems in the Production environment are within the scope of these change control policies and procedures:

- 2nd Wave
- PeopleSoft
- eCenter
- WebAdmin
- eApplication

SDLC Management System

Changes to both Production and support systems are tracked using one or in some cases two change control databases: the Remedy Action Request System and the SDLC Management System. The SDLC Management System currently consists of an Excel spreadsheet called "2W-PS8 Bug List" and an Outlook public folder called "Software Migrations". The Action Request System is used by Support Services and IT staff for tracking help requests and change requests. Change requests that originate outside the EIS group are entered into the Remedy tracking system. If a change request is for a simple application change, as defined by Appendix D: Receiving and Evaluating a Project Change Request, it remains in the Remedy system and is closed when the change has been verified as being completed to the requester's satisfaction. If the change is determined to be a complex or project level change, then the change is entered in the SDLC Management System and tracked using that system.

When EIS is preparing software changes (including PeopleSoft patches, bundles, etc.), the changes are tracked using the SDLC Management System, since these changes must go through the SDLC methodology.

Non-Emergency Change Control Policies

This section addresses overall software change control policies established by Westaff's IT department. Specific procedures to follow when dealing with requested changes are located in the Change Control Procedures section.

Change Review and Approval

Before significant analysis and development work is done on a requested change, the change is evaluated. Changes are evaluated against the criteria listed in Appendix D: Receiving and Evaluating a Project Change Request to determine the change's complexity level.

Requested changes are reviewed at various points through the SDLC process. Appendix F: Required Approvals for Changes is used to determine what approval is needed at various points in the SDLC process to move the change into the next SDLC phase.

Access

Developers will have full read/write access to servers, applications, and databases in the Development environment.

Developers will not have write access to change code, operating systems, databases or applications in non-Development environments. Developers can change data in non-Development environments through the applications by using test user accounts. When troubleshooting problems, developers will work beside business analysts, QA, core engineers, or database administrators who do have write access to the environment.

Once a fix has been developed for a bug, business and/or QA analysts will test the change in a Test environment. If new bugs are discovered during the testing phase, the bugs are logged in the SDLC Management System. The results of the testing will be logged in the SDLC Management System. This logging will include who did the testing and whether the change passed in testing.

If the bug is caused by missed actions or instructions, the Migration Request Form (MRF) is updated with the missing information.

Testing

Whenever possible, initial troubleshooting of bugs reported by field and corporate users is done in a Test environment by business analysts and/or QA analysts. If the analysts are unable to recreate the bug, a developer will try to recreate the issue in a Development environment.

Before a software change is brought up for discussion at the Migration Approval meeting, all necessary testing (including functional, system, regression, and performance testing as deemed necessary by the QA Manager or designee) for each change has been completed in the applicable Test environment(s) and all required communication material has been drafted, approved, and is ready for publication.

When a change is migrated into Production, a validation test is conducted to ensure that the migrated change is the same change as was successfully tested in the Test environment. What kind of testing is necessary to validate the migration depends on what is being migrated as described below:

- For 2nd Wave or other executables, successfully testing the functionality of any one change in that executable is considered adequate to validate that all the other changes in that executable were successfully migrated. This testing confirms that the version of the executable that was migrated is the same version in which testing in the Test environment confirmed changes were successfully implemented.

- For Peoplesoft changes, successfully testing the functionality of the change or finding no significant differences when comparing the objects that make up the change in Production and in the source environment are considered adequate to validate the change was successfully migrated.
- For report changes, successfully generating the report and identifying evidence that at least one of the desired changes is in the report is considered adequate to validate the change was successfully migrated. This testing confirms that the version of the report that was migrated is the same version in which testing in the Test environment confirmed changes were successfully implemented.
- For SQL changes, evidence must be found that the SQL was executed. This evidence can take the form of before and after counts and/or seeing the effects of the SQL's execution through the GUI or through a database tool such as Toad.
- For database changes, evidence must be found that the database change was executed. This evidence can be by seeing the effects of the SQL's execution through a database tool such as Toad.

Migrations

Depending on the type of the change, the source code for the change will be taken from different locations as shown in Table 1.

Change Type	**Where change is staged prior to test**	**Where changes is staged prior to Production**
PeopleSoft Project	Development environment	In Test environment used for system testing
Executable or Service (Changes installed via .msi)	In staging folder	In staging folder
SQL or other flat file (for 2nd Wave)	Team Foundation Server	Team Foundation Server
SQR, SQL, or other flat file (for PeopleSoft)	Development environment	In Test environment used for system testing

Table 1: Source Location for Migrations

Only Core Engineers and Database Administrators have the ability to write changes in the Test and Production environments. Consequently, any changes being migrated to the Production environment must be migrated by the Core Engineering or DBA groups.

If a change requires a complex migration, QA will create a migration plan and request Core Engineers and/or Database Administrators to migrate the change to the Test environment. In the event that migrating the change requires significant coordination between two or more groups or individuals, a migration checklist is created that lists the tasks to be completed as part of the migration, who is responsible for each task, the estimated start time of the task, and what time the task was actually completed.

If the migration requires significant coordination between two or more individuals or groups then one or more migration walk through meetings will be held to walk through the migration checklist.

Emergency Change Control Policies

This section defines the policies and procedures to be used for emergency changes.

The definition of an Emergency Change is as follows: A change made to restore previously working core business functionality. This includes but is not limited to the following: network communication, Westaff's public web site, 2nd Wave, PeopleSoft, eCenter, and Outlook.

Wherever possible, the same policies and procedures used for standard changes will be used for emergency changes. However, often the loss of core functionality causes significant hardship to those affected and must be resolved as soon as possible. Due to the heightened need to speedily resolve the problem addressed by the emergency change, the exceptions listed below are permitted to the standard change control policies and procedures.

1. If possible without causing undue delay, the cause of the problem will be identified prior to creating a solution to the problem. If the cause of the problem cannot be found in a timely manner, a change may be implemented to resolve the immediate consequence(s) of the problem. In such cases, the cause of the problem may be identified when more time is available.
2. Wherever possible, the proposed change to solve the problem will be tested in a non-Production environment in which the problem can be recreated. The purpose of this testing is to (1) confirm that the proposed change does solve the problem, and/or (2) the proposed change eliminates or mediates the consequence(s) of the problem.
3. Wherever possible, if the problem cannot be reproduced in a non-Production environment, the proposed change should be tested to confirm the change does not introduce other problems.
4. If the IT/IS person to approve the changes deems necessary, the change may be implemented in Production without prior testing. Before implementing an untested change in Production, the parts of the system likely to be affected by the change may be backed up in case the change needs to be rolled back and the system restored.
5. The emergency change can be migrated to or implemented in Production during business hours. If necessary, users of the system requiring the change will be logged out of the system in order to enable the change to be implemented.

6. The problem and change to solve or mitigate the problem will be documented in Remedy if the change is a simple change or in the SDLC Management System if the change is a complex change.

7. When time permits, the VP of IS or designee will approve the change prior to its migration to production. If, based on the judgment of those responsible for implementing the change, time does not permit, the change will be migrated to production without the VP of IS' or designee's express approval. In such cases the VP of IS or designee must review and approve the change within the applicable recording system (Remedy/SDLC Management System) within one business day.

8. Once the change is in Production, whenever possible, the change will be implemented in the other environments to maintain synchronicity between the environments.

Non-Emergency Change Control Procedures

For a mid-level view of the change control business flow, see the SDLC Cross Functional Process Flow on the Insider. In the flow certain items are formatted with a black field and white text. For each of those items, a detailed explanation is provided below.

Page 2 – Create CR in SDLC Mgmt Sys
An entry is created in the SDLC Management System for the proposed change. The entry includes the person who requested the change and what the requested change is. If the proposed change is a result of a Remedy change request, the Remedy change request number is entered in the SDLC Management system and the SDLC Management system change identifier is entered in Remedy.

Page 2 – Approve Change
At the next Change Prioritization meeting, the proposed change is discussed by representatives from each group within EIS. For changes that are approved, a priority is assigned to each change using the guidelines provided in Appendix E: Priority Evaluation Criteria. Either during the meeting or immediately thereafter, the proposed change in the SDLC Management system is updated with the priority and its status.

Page 2 – Updates Remedy ticket
For change requests that are rejected, a business analyst updates the Remedy ticket with a suggested message explaining why the request was rejected. Once updated, the ticket is assigned to Support Services who is responsible for communicating the message to the requester.

Page 3 – Update Remedy
For requests that began in the Remedy system, an entry is made in the ticket to indicate the requested change has been approved and prioritized. The work to analyze, develop, test, and implement the change into Production will be done as resources allow. The ticket is then assigned to Support Services.

Page 3 – CR needs Exec Mgmt review
For change requests that would require resources greater than the Director of EIS can approve, using the guidelines provided in Appendix F: Required Approvals for Changes, and/or a policy decision, the proposed change is escalated to Westaff executive approval.

Page 3 – Assign direct to Dev
For requested changes in which the code requirements are self-evident, the request can be sent directly to the Director of EIS. In this case a business analyst is not needed for analysis and a functional requirement specification document is not created.

Page 3 – Assign to Vendor
For requested changes that require changes to software controlled by vendors, the request may be sent to the applicable vendor if required. A Business Analyst will periodically review vendor's progress.

Page 4 – Do Additional Analysis
Before doing analysis, the business analyst refers to Appendix F: Required Approvals for Changes to determine whether additional approval is needed from Director of EIS.

Page 4 – Update CR in SDLC Management system
If the Director of EIS decides to holds the requested change and approve it for development at a later date, comments to that effect are entered in the SDLC Management system.

Page 4 – Does CR need specs
Once additional analysis has been completed, the business analyst determines whether the change requirements are self-evident or not. If the requirements of the change are obvious, the change is forwarded to the Director of EIS for approval. If the change requirements are not obvious, a functional requirements document must be created to provide necessary information to developers and testers.

Page 4 – Have spec walkthrough mtg
Once the needed functional requirement document has been created, the document's author conducts a meeting with business analysts, developers, and QA to walk through the requirements. The meeting's purpose is to clearly state the change's requirements, to resolve questions and concerns related to the change, and to make sure the requirements are understood by developers and testers.

Page 4 – Create/Revise Requirements
For changes in which the code and test requirements are not self-evident, a functional requirements document is created. The document specifies the requirements that must be met in order for the change to be successfully implemented.

Page 4 – Update CR in SDLC Management System
To show approval for development to begin coding a change, the Director of EIS records that approval in the SDLC Management System. This approval can be by e-mail or by an entry directly in the system.

Page 5 – Developer Create/update Migration Request
Once the developer has finished coding the requested change, the developer completes an MRF to request the change be migrated into a non-Development environment. The MRF should provide enough information for Core Engineers and/or DBAs to migrate the change into test and later Production environments.

Page 5 – Update CR in SDLC Mgmt Sys
After the MRF has been reviewed for completeness, the QA Manager or designee updates the SDLC Management System by requesting DBAs and/or Core Engineers migrate the change into one or more designated Test environments.

For offline files such as SQLs, SQRs, nVision templates, and executable files, the files should be moved into a folder to which developers do not have read/write access. This is to ensure that the files that are tested are not changed after they pass the testing phase but before they are migrated to Production. Prior to moving the files in the staging area, the QA Manager or designee should verify the version listed in the MRF matches the version number of the file to be staged.

For PeopleSoft changes, the files can be staged in the Development environment for migrations to a Test environment.

Use the following guidelines when choosing a Test environment:

- As a general rule, emergency changes and changes to data should be migrated to and tested in the most recently refreshed environment that most closely matches Production.
- Changes being released together with other changes should be migrated to the environment designated for testing the set of changes. For 2nd Wave changes, migrate to both Upgrade and Conversion.
- For report, FOG, eApp, Elise, and Outlook integration changes, select Upgrade.

Page 5 – Update SDLC Mgmt Sys
Send e-mail confirming success or indicating failure.

Page 5 – <u>Tester</u> Update CR in SDLC Mgmt Sys with test results
In the change's entry, the tester should summarize testing done (duration, conditions, frequency, test process, type of regression testing, problems encountered). The tester should also indicate risks of migrating change.

If testing is for a Major Project change, the testing should include parallel testing in which test system output is compared to corresponding production output. The testing should also include User Acceptance Testing in which business users use the test system and validate it supports required business operations.

Page 5 – <u>Bus. Owner</u> Approve change
If a business owner requested the change, the business owner should send an e-mail stating approval of the change to be migrated to Production.

Page 6 – Update SDLC Mgmt Sys
Check that the system has entries approving the migration. Enter the migration plan or a link to the plan in the system.

Page 6 – IT Mgmt Approve Migration
Each software change (whether application or OS/patch) to be migrated to Production is reviewed at the Migration Approval meeting. Before a change is brought up for discussion, all necessary testing for each change is completed and all required communication material has been drafted, approved, and is ready for publication. The person(s) who tested the change, or designee, is present in the meeting to explain how the change was tested. During the meeting, each proposed change is discussed and IT management determines which changes are approved to be migrated. IT management also determines whether the change will be migrated on Thursday or on a Saturday. Any upcoming hardware changes are also announced so that their implementation can be coordinated, if appropriate, with software changes.

After the meeting, the QA Manager or designee will send e-mail listing IT management's verbally approved changes to the VP of IS or designee and CC the rest of the IT managers.

Page 6 – Support Services Announce upcoming changes
After the VP of IS or designee has replied with written approval, a maintenance notification is prepared and sent to Support Services if end users are affected by the migration. Support Services then issues an email message announcing the upcoming changes—whether or not any outage of service is expected. Any additional written communication prepared to announce the change is also issued by Support Services. All such communication should be published with a minimum of two business days advance notice.

Page 6 – Migrates System to Prod
Before migrating a change, backups are taken of affected database tables in case the change needs to be rolled back.

Page 6 – Complete Migration Plan
The QA Manager or designee completes a migration plan that lists the change(s) being migrated to Production and provides links to the MRFs or other source information for each change. If the migration requires coordination between multiple people, a migration checklist is also prepared that lists the tasks to be accomplished in chronological order, who is to complete the task, and when the task is expected to begin. The checklist should be a shared Excel spreadsheet so that multiple people can view and make changes to the checklist during the migration.

Changes are generally migrated to Production on Thursday, Friday, or Saturday.

Page 6 – Tester(s) Validate change in Prod
Once the change has been migrated into the Production environment, a validation test should be performed to (1) verify that the change was successfully migrated to Production and (2) that migrating the change did not cause problems. Since the change is now in Production, care should be taken to not cause data to be written to the database, e.g., saving a record. Acceptable tests include running searches and reports, viewing the software version number, viewing GUI

changes, comparing files between Prod and test to verify only environment-specific settings are different between the two files. Once the tester completes validation testing, an entry should be made in the SDLC Management System indicating the results of the testing.

Page 6 – Update/Close CR in SDLC Management Sys
Once the migration is complete, the change request entry in the SDLC Management System should be reviewed to ensure required approvals have been noted in the system and the change is marked as Closed.

Scheduling/Timing

Unless the complex change is an emergency change, the following general events shown in Table 2 should be completed before the change is moved into Production.

Emergency bug fixes or simple bug fixes and enhancements can be migrated on days other than Thursday or Saturday/Sunday depending on resource availability and urgency.

When *	**Event**
Mon/Wed	Change Review Meeting Changes entered into the SDLC Management System are reviewed in a meeting attended by business and QA analysts and developers. Changes are rejected or accepted and prioritized.
As needed	One or more changes are grouped into a release. The changes in a release are generally migrated together into the Production environment.
Wed	Migration Approval Meeting Software (both application changes and OS patches) and hardware changes planned to be migrated to the Production environment are reviewed by the IT managers or their designees and approval is gotten from the VP of IS or designee. A Scheduled Maintenance Form is created and submitted by the Tuesday before the planned migration. If the migration affects field users or a large number of corporate users, Support Services announces the upcoming changes.
Wed	Migration Plan Walkthrough If management deems necessary, a walkthrough meeting is held to walk through the migration plan.
Thu	If the change(s) can be migrated to Production within the maintenance period, IT migrates changes into Production environment and tests to ensure changes were migrated properly.

Sat	If the change(s) require a longer window to migrate, the changes are migrated during the maintenance period beginning on Saturday. IT migrates changes into Production environment and tests to ensure changes were migrated properly.

Table 2: General Change Migration Event Schedule

* Days subject to change. In the case of large and/or complex changes, it is expected that several Migration Plan walkthroughs will need to be created.

Emergency Change Control Procedures

The following procedures will be used to implement emergency changes in the Production environment.

1. Upon becoming aware of the problem, the person noticing the problem either reports the problem to Support Services or contacts EIS directly.

   If contacted directly, EIS will contact Support Services, if appropriate, to create a Remedy ticket and/or announce the problem so that others are aware that EIS is working on resolving the issue. In this case, steps 2 through 4 are skipped.

2. Support Services creates a Remedy ticket and try to solve the problem.

3. If unable to solve the problem, Support Services contacts a person within the group responsible for the functional area in which the problem is appearing and alerts that person to the problem.

4. Support Services routes the Remedy ticket to the individual or group responsible for the functional area in which the problem is appearing.

5. One or more people within the group assigned analyze the problem to determine root causes and/or solutions to mitigate the problem. If necessary, additional individuals and groups are called in to assist. As part of this analysis, the problem is recreated in a non-Production environment.

6. Once the preferred solution has been identified, an MRF is created, if needed, and QA reviews the request. After approving the request, QA creates a migration plan, if necessary, and requests the change be implemented in a Test environment.

7. Core Engineering and/or DBAs migrate the change to the designated Test environment.

8. Once testing has been satisfactorily completed, or determined to be unnecessary, a request for migration approval is made via e-mail, so that the approval can be documented. The request is addressed to IT-Management and the body of the message includes the following:

   - A summary of the problem

- How the problem is being fixed
- What testing was done to validate the change
- The intended timeframe in which the change is to be implemented in Production.

If e-mail is not immediately available, the approver can verbally approve the change and then respond to the e-mail when it is available.

9. Wherever possible, the approval e-mail is forwarded to the IS group(s) responsible for implementing the change. List-is-service-request, prodenvchanges@westaff.com and QA Migrations are courtesy copied in the same e-mail. Support Services documents the change in the Remedy ticket and includes the request and approval e-mail in the Remedy ticket.

10. If a migration plan is necessary, the approver forwards the request to QA who creates the migration plan.

11. Core Engineering and/or DBAs migrates the change into the Production environment.

12. Core Engineering, DBAs, and/or Support Services monitor Production to determine whether the migrated change had the intended effect and whether any additional problems were caused by the migration.

Backups

This section provides the policies and procedures related to creating and verifying data backups in Westaff's Production environment.

Policies

Support Center receives emails daily from Networker and scripts written to automate the notifications. The email notification contains successes and failures as they relate to Westaff Production backups. Support opens a Remedy ticket and assigns it to IT SE for an Engineer to review and close.

The reviews are logged into Remedy using the CTI below:

- Category = Software
- Type = SOX
- Item = Backup Review

Procedures

The EMC Networker software is set up to send all server backup information to the list-is-service-request distribution list daily. Support Center monitors this list daily and opens a Remedy ticket, copies all failures and only successes for the following EMC Networker groups:

- DC1_3mPSOFT_1
- DC1_3mPSOFT
- DC1_3mARCHREDO
- DC1_MntlyPSOFT
- DC1_MntlyPSOFT_1
- DC1_3mHP
- DC2_3mMSFT_1
- DC2_Mnthlymsft_1

A script runs daily and sends an e-mail to list-is-service-request distribution list if the EUC files were copied or not. The Support Center adds this information to the Remedy ticket mentioned above. The ticket is assign to List-IT SE. An IT Engineer researches failures and documents the steps taken to remedy the failure if any and closes the ticket acknowledging that it has been reviewed.

- See Appendix B for EMC Networker group details.

Disaster Recovery

This section provides the policies and procedures related to verifying restores of Westaff's Production systems and data in a non-Production environment.

Policies

Production 2nd Wave data and PeopleSoft application and data are backed up on a daily basis. In the event of a disaster, these backups would be used to restore 2nd Wave data and PeopleSoft application and data into a non-Production environment. Once the restore is complete, the environment would become the interim Production environment, while the full capability of the Production environment is restored.

To validate that the interim environment can be created within a timely basis, a test database is refreshed using the daily backups.

Procedures

Backups of the Production 2nd Wave and PeopleSoft systems are made on a daily basis. The procedures below are used to validate the ability to recover Production 2nd Wave and PeopleSoft data.

One or more DBAs will use the Production backups for a specified day and restore 2nd Wave data and the PeopleSoft back office system into a designated non-Production environment.

When the DBAs have finished restoring the 2nd Wave data, a Business Analyst or designee runs a query in the restored 2nd Wave database's timecard table to generate a spreadsheet listing all the timecards entered for a given day. The Business Analysts or designee runs the same query on the Production 2nd Wave database.

The totals for each column in the two spreadsheets are compared. Identical amounts in the corresponding columns of the spreadsheets are accepted as proof that the database values in the restored database match the values in Production.

When the DBAs have finished restoring the PeopleSoft systems, Business Analysts or designees use the application to generate a list of payroll reports in the HCM system and general ledger reports in the FMS systems. The same reports are generated for the same day using the Production HCM and FMS systems. The HCM reports and the FMS reports are compared. Identical totals in the corresponding systems are accepted as proof that the database values in the restored systems match the values in Production.

For the SFO system, a Business Analyst or designee runs a query in the restored SFO database and generates a spreadsheet listing the query's results. The same query is run on the Production SFO database and again generates a spreadsheet listing the query's results.

The totals for each column in the two spreadsheets are compared. Identical amounts in the corresponding columns of the spreadsheets are accepted as proof that the database values in the restored database match the values in Production.

The Remedy system is used to document the restore. A Remedy ticket is created and relevant files are attached to the ticket.

Appendix A: Information Service Personnel Listing

The following chart shows the current position holders by referenced IT titles.

IT Title	**Name**	**Login**
Vice President, Information Services	Andy Elgazzar	aelgazzar
Director, Enterprise Information Services (Interim)	Louisa Garrido	lgarrido
Information Technology Manager	Ann Crommie	acrommie
Quality Assurance Manager	Jim Driggers	jdriggers
Database Administrator	Robert Wallace	rwallace
Information Technology Engineer	Candace Memmott	cmemmott
Information Technology Engineer	Doug Meahan	dmeahan
Information Technology Engineer	Rob Hutter	rhutter
Information Technology Engineer	Matt Fox	mfox
Network Engineer	Todd Taylor	ttaylor

Appendix Change History

Date	By	Action	Approved
2/4/09	Jim Driggers	Added Louisa Garrido and (Interim) to Director, Enterprise Information Services Replaced "Director, IT Operations" with "VP of Information Services"	

Appendix B: Legato Groups

The following chart shows the Legato groups whose successfully backup each day is reviewed.

- DC1_3mPSOFT_1
- DC1_3mPSOFT
- DC1_3mARCHREDO
- DC1_MntlyPSOFT_1
- DC1_3mHP
- DC2_3mMSFT_1
- DC2_Mnthlymsft_1

Group Name - DC1_3mPSOFT_1:

Server	**Function**	**Frequency**
DC1XDB01	Production PeopleSoft database	Full backup on Saturday except for the first Saturday of the month and incremental every other day of the month

Group Name - DC1_3mPSOFT:

Server	Function	Frequency
DC1BH01	Production PeopleSoft batch server	Full backup on Saturday except for the first Saturday of the month and incremental every other day of the month
DC1BH02	Production PeopleSoft batch server	Full backup on Sunday except for the first Sunday of the month and incremental every other day of the month
DC1XAP01	Production PeopleSoft application server	Full backup on Saturday except for the first Saturday of the month and incremental every other day of the month
DC1XAP02	Production PeopleSoft application server	Full backup on Sunday except for the first Sunday of the month and incremental every other day of the month
DC1XWB01	Production PeopleSoft web server	Full backup on Saturday except for the first Saturday of the month and incremental every other day of the month

DC1XWB02	Production PeopleSoft web server	Full backup on Sunday except for the first Sunday of the month and incremental every other day of the month

Group Name - DC1_3mARCHREDO

Server	Function	Frequency
Belize	2nd Wave database	Full daily of redo logs

Group Name - DC1_MntlyPSOFT_1

Server	Function	Frequency
DC1BH01	Production PeopleSoft batch server	Every first Saturday of the month
DC1BH02	Production PeopleSoft batch server	Every first Sunday of the month
DC1XAP01	Production PeopleSoft application server	Every first Saturday of the month
DC1XAP02	Production PeopleSoft application server	Every first Sunday of the month
DC1XWB01	Production PeopleSoft web server	Every first Saturday of the month
DC1XWB02	Production PeopleSoft web server	Every first Sunday of the month

Group Name - DC1_MntlyPSOFT_1

Server	Function	Frequency
DC1XDB01	Production PeopleSoft database	Every first Saturday of the month

Group Name - DC1_3mHP

Server	Function	Frequency
Belize	2nd Wave database	Full backup on Sunday except for the first Sunday of the month and incremental every other day of the month

Group Name - DC2_3mMSFT_1

Server	Function	Frequency
Sigma	Production file server	Incremental everyday except for the 1st Saturday of the month

Group Name - DC2_Mnthlymsft_1

Server	Function	Frequency
Sigma	Production file server	Full on 1st Saturday of the month

Appendix Change History

Date	By	Action	Approved

Appendix C: EUC File Review

The following files are considered Confidential. Access to these files is restricted and reviewed on a semi-annual basis.

Filename	Area
Provision [Qtr] [Year]_FINAL.xls	Tax
[Year] Tax Provision_FINAL [Date].xls	Tax
Billing Adjustments Reserve.xls	Credit/AR
Experience Modifier Calculation.xls	GL
Workers Comp and General Liab Reserve Analysis [PD] [Year].xls	GL
Various files and supporting schedules that support these final documents: Form 10Q [qtr] version [number].doc, MS Word Document version of Q1 08 Form 10Q.doc	GL
Various files and supporting schedules that support this final document: FINAL 10-K word document (from Merrill Corp).doc	GL
PD[period][year].xls	GL
Various Commissions calculation spreadsheet	GL

Appendix Change History

Date	By	Action	Approved
10/29/08	Jim Driggers	Added "Various Commissions calculation spreadsheet" and GL row to table.	Mark Bierman

Appendix D: Receiving and Evaluating a Project Change Request

Use the following table to guide evaluation of change requests. Simple changes are shown in light gray, while complex changes are shown in darker gray. The kind of change is determined by comparing the characteristics of each category. The column which contains the rightmost category characteristics best describing the change is considered to be the change's level.

Category	**Support Services** **Tracked in Remedy**	**Business Analyst** **Tracked in Remedy**	**Developer** **Tracked in SDLC Management System**	**Project (1)** **Tracked in SDLC Management System**	**Major Project (2)** **Tracked in SDLC Management System**
Database structure or executable	N/A	Does not require developer/DBA to change executable or database structure.	Does require developer/DBA to change executable or database structure.	Does require developer/DBA to change executable or database structure.	Replaces database architecture; physical change of server(s) location; replacement of front/back office system
Modifying data	Change will be made through GUI	Change will be made through GUI or will be made using previously tested and verified means of generating SQL statements. (3)	Change will be made using previously untested SQL/SQR script or Datamover script to modify data. Setting/modifying global setup parameters.	Change will be made using previously untested SQL/SQR script or Datamover script to modify data. Setting/modifying global setup parameters.	Requires conversion of data from one database version or type to another database version or type.

Category	**Support Services** **Tracked in Remedy**	**Business Analyst** **Tracked in Remedy**	**Developer** **Tracked in SDLC Management System**	**Project (1)** **Tracked in SDLC Management System**	**Major Project (2)** **Tracked in SDLC Management System**
Communication	Change can be effected by one group.	Change can be effected by one group.	Change requires interaction between two or more groups.	Change requires interaction between two or more groups.	Change requires extensive interaction between two or more groups.
New Patch or Upgrade from Vendor	No	No	Yes	Yes	Yes
Security	Granting existing roles/profiles to a user.	N/A	Adding/modifying a role/profile.	Adding/modifying a role/profile.	Widespread significant changes to many roles/profiles.
Requirements	Simple requirements that can be gotten via phone call, e-mail, in person visit	Request specifies requirements in sufficient detail to implement change.	Additional analysis required to clarify request's requirements and documented in Functional Spec.	Additional analysis required to clarify request's requirements.	Requires extensive analysis and design with approval from Westaff Executives
Time (Person-hours)	< 4 hrs	< 8 hr	<40 hrs	40+ hrs	> 3 months

Category	**Support Services** **Tracked in Remedy**	**Business Analyst** **Tracked in Remedy**	**Developer** **Tracked in SDLC Management System**	**Project (1)** **Tracked in SDLC Management System**	**Major Project (2)** **Tracked in SDLC Management System**
Visibility/ Audience	Single user	Single branch/office	Multi branch/office	Enterprise wide	Enterprise wide

(1) Requires Business Sponsor and identification of cost center(s) to which charge costs

(2) Requires Executive Sponsor and allocation of project-specific funding

(3) Examples of these would be scripts to add marketing information, new offices, or burden rates updates in 2nd Wave's database

Appendix Change History

Date	By	Action	Approved
2/4/09	Jim Driggers	Added column for Major Project and modified characteristics of Project and Major Project change types. Clarified characteristics for Modifying Data category	

Appendix E: Priority Evaluation Criteria

Use the following list of criteria when evaluating bug and enhancement change requests.

Type	Criteria
1 – Critical	Bug that could cause loss of core business functionality in one or more offices/departments.
2 – High	Bug that significantly impairs a large number of offices/departments. A workaround exists, but is insufficient for long-term use.
3 – Normal	Bug that impairs few offices/departments or has an easy workaround.
4 – Low	Bug that affects a few users and does not cause loss of business functionality.

Table 3: Bug Evaluation Criteria

Criteria	Enhancement
1 – Critical	As determined by management.
2 – High	As determined by management.
3 – Normal	As determined by management.
4 – Low	As determined by management.

Table 4: Enhancement Evaluation Criteria

Appendix Change History

Date	By	Action	Approved

Appendix F: Required Approvals for Changes

Before any changes can be migrated into Production those changes must be approved. Use the following tables to determine what level of approval is needed to advance the change and supporting documentation through the various SDLC stages.

Required Approvals for Significant Analysis

Use Table 5 to determine what level of approval is needed before significant time is spent analyzing and/or developing a solution to satisfy a change request. In determining what level of authority is required, use the column which best describes the change overall. For example, if the change is a complex change, but has no costs (associated with purchasing hardware, software, or consulting services) and requires less than one day to develop and test, then the business analyst can decide whether the change should be implemented.

Regardless of what level is required to approve analysis and development efforts, additional approvals are needed before the change can be migrated into Production.

Category	**Support Services**	**Business Analyst**	**Director of EIS**	**VP of IS or designee**
Complexity	Simple	Simple	Complex	Complex
Cost (1)	$0	$0	< $10,000	> $10,000
Development/Testing Time Required (2)	None	< 1 day	< 3 week	> 3 week

Table 5: Approval Level Required before Significant Analysis Begins

(1) Cost does not include cost of Westaff personnel.
(2) Calculated using one person's 40 hour work week

Change Approval Matrix

The following matrix show the documents that need to get created and approved by role and when for complex changes in the software development process.

Document	Prior to Development	Prior to Test	Prior to Production
Create Change Request	Business Analyst Developer QA Analyst		
Approve Change Request	Director, EIS		
Create Test Migration Request Form		Developer	
Approve Test Migration Request Form		QA Manager (1)	
Create Production Migration Request		QA Manager (1)	
Approve Production Migration Request			VP of IS (1)
Approve Production Migration for Major Project (2)			VP of IS or designee (1) Executive Sponsor Business User Manager

(1) Or designee

(2) If change is a Major Project, VP of IS, Executive Sponsor(s) (if any) and Manager(s) of business users affected by change must approve before change is implemented in Production. Such approval indicates approval of User Acceptance Testing.

Table 6: Approvals for Software Development

Appendix Change History

Date	By	Action	Approved
1/5/09	Jim Driggers	Added Notes 1 and 2 Removed CIO entry. Replaced “Director of IT” with “VP of IS” Changed “Approve Production Migration Request” to require VP of IS.	

Appendix G: Generic Domain Accounts

The table below shows the generic domain accounts that have been set up for administrative purposes in the indicated PeopleSoft areas.

User ID	Purpose	Used By	Domain	OS	Database	Application
BATCHJOB	Used for scheduling PER099	HCM Business Analyst			HCM	HCM
LDAP		Used by the application			HCM	HCM
PSAPPS	Used for interfacing 2nd Wave to PeopleSoft	Used by the application			HCM	HCM
PTWEBSERVER	The PTWEBSERVER domain account provides the portal servlet with minimal security access. Users cannot logon into PS if this userid is locked.	Used by the application			HCM	HCM
BATCHJOB	Used for scheduling jobs and billing cycle	FMS Business Analyst			FMS	FMS

User ID	Purpose	Used By	Domain	OS	Database	Application
BatchRpt_AR_Aging	Used for defining, maintaining and scheduling Affiliate GL Detail Crystal Reports. Also, currently used to schedule GL_JEDIT - Batch Journal Edit job. Additional, Support Center uses this domain account for the Aging Report (Crystal) maintenance.	Support Center, Business Analyst			FMS	FMS
LDAP		Used by the application			FMS	FMS
PSAPPS	Used for interfacing 2nd Wave to PeopleSoft	Used by the application			FMS	FMS
REPORTUSER	Used for defining, maintaining and scheduling nVision Report Books for GL Detail, Income Statement and Trend graph reports.	Peggy Davis (accountant), Business Analyst			FMS	FMS
PTWEBSERVER	The PTWEBSERVER domain account provides the portal servlet with minimal security access. Users cannot logon into PS if this userid is locked.	Used by the application			FMS	FMS
PSAPPS	Used for interfacing 2nd Wave to PeopleSoft	Used by the application			SFO	SFO

User ID	Purpose	Used By	Domain	OS	Database	Application
PTWEBSERVER	The PTWEBSERVER domain account provides the portal servlet with minimal security access. Users cannot logon into PS if this userid is locked.	Used by the application			SFO	SFO

Domain accounts not based on user's first name initial and last name do exist and are used by Core Engineering for troubleshooting purposes. These accounts are assigned on a one-to-one basis to Core Engineers identified in AD. These domain accounts do not have access to 2nd Wave or PeopleSoft.

Appendix Change History

Date	By	Action	Approved

Appendix H: EUC Folder Structure

End User Computing files are contained in the following secured folder structure. The personnel who control access to each folder are listed after the folder name.

The folder structure is **\\dc2nas04\restrictedaccess** and the files beneath it are:

- WorkersComp folder- Nancy Sifter
- Financials folder - Sean Wong
- Credit folder - Maureen Caslavka
- Incentives - Leah Vitalicio

Appendix Change History

Date	By	Action	Approved
10/29/08	Jim Driggers	Removed Tax Folder from list. This folder was removed by business manager's request from restricted access. Removed ForeignCalculations folder from list. Added Incentives folder.	Mark Bierman
2/4/08	Jim Driggers	For Financials folder, replace Cecilia Minalga with Sean Wong	

Appendix I: Periodic Review Schedule

In the table below, rows displayed in regular text refer to reviews of the policies and procedures themselves. Rows displayed in italicized text refer to reviews in the Production environment made to validate policies and procedures implementation.

		Dates				
Policy	**Reviewed By ***	**Policy Effective**	**Implemented**	**Last Review**	**Next Scheduled Review**	**Frequency**
Network and Application Access	VP of IS	8/25/08	1/1/08	8/7/08	8/25/09	Yearly
Inactive Domain Account Review	*Support Services*	8/25/08	7/7/08	2/2/09	5/2/09	*Quarterly*
Developer/DBA Access Review	*Director EIS*	8/25/08	7/1/08	10/30/08	4/30/09	*Semi-annual*
EUC Access Review	*See Note 1*	8/25/08	7/7/08	10/31/08	4/30/09	*Semi-annual*
Operating System Access Review	*IT Manager*	8/25/08	8/26/08	1/2/09	TBD	*Upon CE termination*
PeopleSoft and 2nd Wave Access Review	*See Note 2*	8/25/08	10/17/08	10/31/08	4/15/09	*Semi-annual*
Firewall Monitoring	*VP of IS*	8/25/08	8/13/08	8/13/08	3/13/09	*Annual and upon change request completion*
Wireless Connectivity	*Network Engineer*	8/25/08	---		TBD	*Yearly*
VPN Connectivity	*Network Engineer*	8/25/08	---		TBD	*Yearly*
Password Controls	VP of IS	8/25/08	4/24/08	8/7/08	8/7/09	Yearly
Authentication	VP of IS	8/25/08	1/1/08	8/7/08	8/7/09	Yearly
Data Center Access Review	*VP of IS*	8/25/08	6/26/08	10/15/08	1/15/09	*Quarterly*
Change Control - Patches	VP of IS	8/25/08	1/1/08	8/7/08	8/7/09	Yearly
Change Control - Applications	VP of IS	8/25/08	7/1/08	8/7/08	8/7/09	Yearly
Backups	*VP of IS*	8/25/08	8/18/08	Current day	Daily	*Daily* *See Note 3*
Disaster Recovery	VP of IS	TBD				

* Or Designee

Note 1: EUC file access is reviewed by each person who controls access to a folder containing EUC file(s).

Note 2: PeopleSoft and 2nd Wave user access is reviewed by the employee's Executive or one or more manager designees. For Affiliate user access, 2nd Wave user access is reviewed by the Vice President of Franchise Operations or that person's designees.

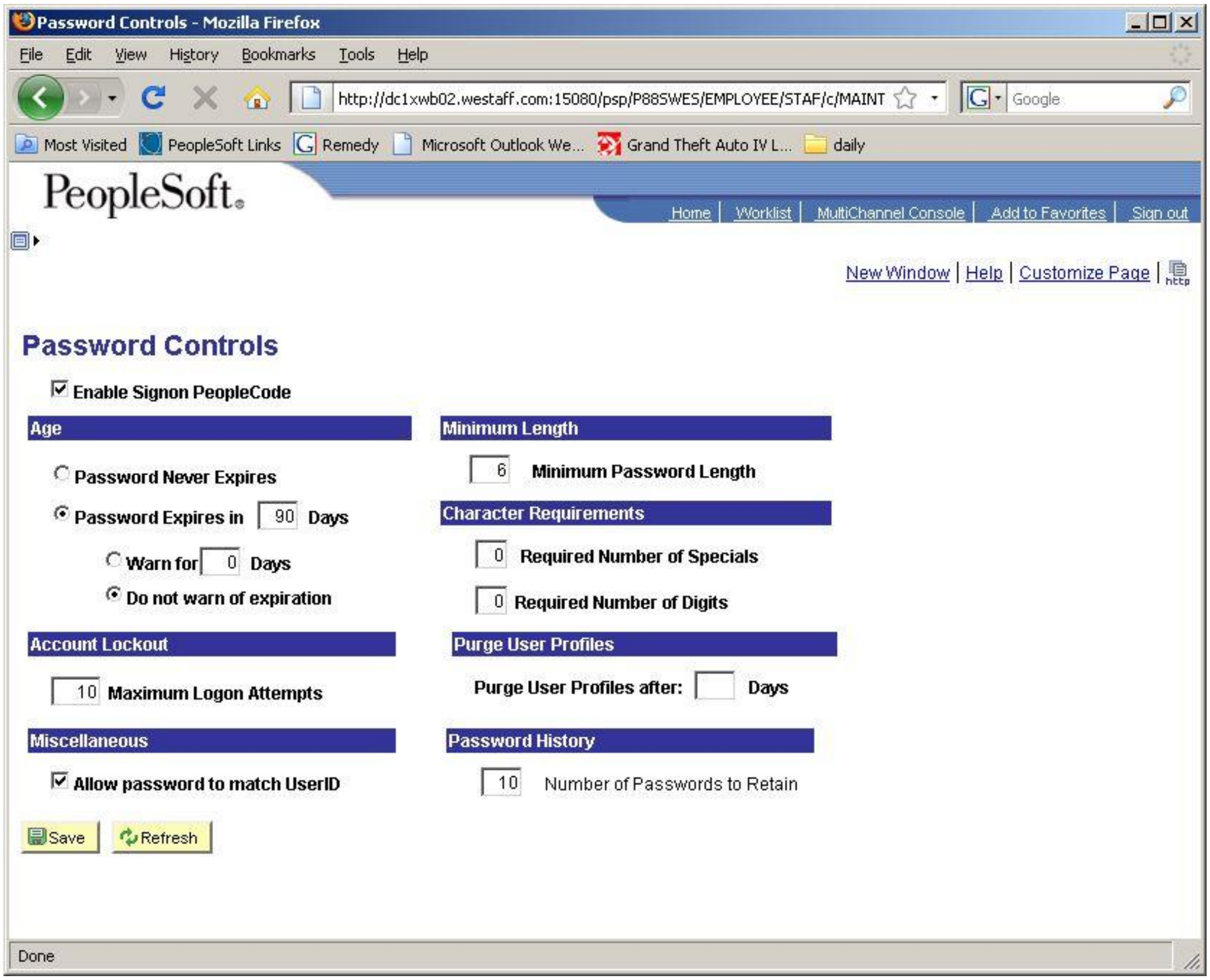
Note 3: Backups are reviewed Monday through Friday.

Appendix Change History

Date	By	Action	Approved
10/27/08	Jim Driggers	Added "Annual" and "3/13/09" to Firewall monitoring Frequency and Next Scheduled Review. Added "8/26/08" to Operating System Access Review Implemented To PeopleSoft and 2nd Wave Access Review, added Implementation date of 10/17/08, Last Review date of 10/31/08, and Next Scheduled Review data of 4/15/09. Deleted Note 4. To Wireless Connectivity and VPN Connectivity, replaced "As Needed" with "Yearly"	Mark Bierman
2/4/09	Jim Driggers	Updated dates throughout table. Added * note "or Designee.	

Appendix J: PeopleSoft Staffing Front Office Security

The screenshot below illustrates the security set up in PeopleSoft SFO.


Password Controls - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://dc1xwb02.westaff.com:15080/psp/P88SWES/EMPLOYEE/STAF/c/MAINT
Google
Most Visited PeopleSoft Links Remedy Microsoft Outlook We... Grand Theft Auto IV L... daily
PeopleSoft.
Home | Worklist | MultiChannel Console | Add to Favorites | Sign out
New Window | Help | Customize Page
Save
Refresh
Done

Password Controls

☑ Enable Signon PeopleCode

Age

○ Password Never Expires

● Password Expires in 90 Days

○ Warn for 0 Days

● Do not warn of expiration

Account Lockout

10 Maximum Logon Attempts

Miscellaneous

☑ Allow password to match UserID

Minimum Length

6 Minimum Password Length

Character Requirements

0 Required Number of Specials

0 Required Number of Digits

Purge User Profiles

Purge User Profiles after: Days

Password History

10 Number of Passwords to Retain

Appendix Change History

Date	By	Action	Approved