Section 300
Office

Remote Access Policy

1.0 Purpose
The purpose of this policy is to define standards for connecting to PA West Soccer's network from any host. These standards are designed to minimize the potential exposure to PA West Soccer from damages, which may result from unauthorized use of PA West Soccer resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical PA West Soccer internal systems, etc.

2.0 Scope
This policy applies to all PA West Soccer associates, contractors, vendors and agents with a PA West Soccer-owned or personally-owned computer or workstation used to connect to the PA West Soccer network. This policy applies to remote access connections used to do work on behalf of PA West Soccer, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy
3.1 General
1. It is the responsibility of PA West Soccer associates, contractors, vendors and agents with remote access privileges to PA West Soccer's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to PA West Soccer.
2. General access to the Internet for recreational use by immediate household members through the PA West Soccer Network on personal computers is prohibited. The PA West Soccer associate is responsible to ensure the family member does not violate any PA West Soccer policies, does not perform illegal activities, and does not use the access for outside business interests. The PA West Soccer associate bears responsibility for the consequences should the access is misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of PA West Soccer's network:
    a. *Acceptable Encryption Policy*
    b. *Virtual Private Network (VPN) Policy*
    c. *Wireless Communications Policy*
    d. *Acceptable Use Policy*
4. For additional information regarding PA West Soccer's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.
5.

3.2 Requirements
1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

2. At no time should any PA West Soccer associate provide their login or email password to anyone, not even family members.
3. PA West Soccer associates and contractors with remote access privileges must ensure that their PA West Soccer-owned or personal computer or workstation, which is remotely connected to PA West Soccer's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. PA West Soccer associates and contractors with remote access privileges to PA West Soccer's corporate network must not use non-PA West Soccer email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct PA West business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the PA West Soccer network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by Remote Access Services, and IT must approve security configurations for access to hardware.
9. All hosts that are connected to PA West Soccer internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to PA West Soccer's networks must meet the requirements of PA West Soccer-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the PA West Soccer production network must obtain prior approval from Remote Access Services and IT.

4.0 Enforcement

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

5.0 Definitions

Term	**Definition**
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a PA West-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into PA West and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
Remote Access	Any access to PA West Soccer's corporate network through a non-PA West Soccer controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-PA West Soccer network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into PA West Soccer's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

PA West Soccer Web Site

PA West Soccer shall maintain a web site as a digital means of communicating with its membership and the soccer community. The purpose of the PA West Soccer web site shall be to promote PA West Soccer and, as applicable, those activities of East Region, US Youth Soccer, and US Soccer.

Webmaster
American Eagle is currently the approved web site designer and web master. The Executive Director or designee shall coordinate all updates of the web site with the webmaster. The Executive Director or designee must approve all changes to the PA West Soccer web site.

Content
Content of the PA West Soccer web site shall focus on the activities and offerings of PA West Soccer. The web site will provide space for the following portions of the organization: Administration/Executive Board, Youth Division, Adult Division, Coaching Development, Player Development, Competition. Each committee or cost center of the association will be responsible for providing the Executive Director or designee with content for their portion(s) of the web site.

News items specific to individual members shall be restricted to those pertaining to PA West Soccer Board members and those members in good standing with a notable achievement within the state association, US Youth Soccer, or the national level of US Soccer.

PA West Soccer shall offer a link between the PA West Soccer web site and our member clubs' web sites when requested. Provided the member offers a reciprocating link from their site to the PA West Soccer site and their web site does not link to material contrary to the mission of PA West Soccer.

Information from non-members, not having a specific tie to PA West Soccer or that which is not of specific importance to PA West Soccer members shall not be considered for posting on the PA West Soccer web site. Links shall not be made to web sites that are sourced from members of PA West Soccer whom are allocated space on the PA West Soccer web site.

Advertising
PA West Soccer can make available for purchase advertising space on its web site. The space shall be limited to one banner ad per page. The cost shall be $400.00 for the banner ad on the Home Page and $300.00 for a banner ad on internal pages. The purchase of ad space would be good for 30 days.

E-Mailing Lists
The PA West Soccer web site offers a subscription service for individuals interested in receiving information via email. The service shall be administered by the Executive Director or designee.

Mailing lists shall include: Coaching Development, Player Development, Youth News, Adult News, State Cup, Open Tournament, Referees, Boys ODP, Girls ODP, and a General list to all subscribers.

Email lists may be rented at a rate of $100.00 per blast. Content is subject to the approval of the Executive Director.

IT Acceptable Use Policy

1.0 Overview

IT's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to PA West Soccer's established culture of openness, trust and integrity. IT is committed to protecting PA West Soccer's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of PA West Soccer. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every PA West Soccer employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at PA West Soccer. These rules are in place to protect the employee and PA West Soccer. Inappropriate use exposes PA West Soccer to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at PA West Soccer, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by PA West Soccer.

4.0 Policy

4.1 General Use and Ownership

1. While PA West Soccer's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of PA West Soccer. Because of the need to protect PA West Soccer's network, management cannot guarantee the confidentiality of information stored on any network device belonging to PA West Soccer.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. IT recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see IT's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to IT's Awareness Initiative.
4. For security and network maintenance purposes, authorized individuals within PA West Soccer may monitor equipment, systems and network traffic at any time, per IT's Audit Policy.
5. PA West Soccer reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.
4. Use encryption of information in compliance with IT's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Laptop Security Tips”.
6. Postings by employees from a PA West Soccer email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of PA West Soccer, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the PA West Soccer Internet/Intranet/Extranet, whether owned by the employee or PA West Soccer, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of PA West Soccer authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing PA West Soccer-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by PA West Soccer.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which PA West Soccer or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a PA West Soccer computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any PA West Soccer account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to IT is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, PA West Soccer employees to parties outside PA West Soccer.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within PA West Soccer's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by PA West Soccer or connected via PA West Soccer's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

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

6.0 Definitions

Term	**Definition**
Spam	Unauthorized and/or unsolicited electronic mass mailings.

Computer System

Overview
PA West Soccer currently uses a server network with workstations. Each user on the network may use any workstation to log onto the network. However, each user will only have access to the programs and files for which they are approved which will be verified through their password. Access to files and the System Administrator (currently the Executive Director) may change programs as necessary. All systems should be backed up nightly to external hard drive and cloud-based storage. Individual users may change passwords whenever they wish but the system will require it every 180 days.

Programs
All programs on the server and individual workstations must be licensed to PA West Soccer and approved by the System Administrator. All computers must have anti-virus programs resident on them which must be kept current as recommended by the manufacturer.

Currently approved software includes the following:

- MS Windows
- MS Office (Excel, Word, PowerPoint and Access)
- Norton Anti-Virus
- Novell
- Quickbooks
- Adobe Reader
- Malwarebytes

Inventory
The System Administrator shall keep an accurate inventory of computer and peripheral equipment. Equipment should be recorded by primary user and should list the manufacturer, model, serial number, PA West Soccer identification number and date purchased (or leased). Equipment removed from the State Office must be approved and recorded by the Executive Director.

Proprietary Information
All information, files and e-mail on PA West Soccer computers are the property of PA West Soccer. Users should not expect that any of this information is private except for personnel and salary information.

Security
Firewalls, passwords, anti-virus programs and disaster recovery systems shall be the responsibility of the Systems Administrator.

Ownership of Mailing Lists
The membership list of players, coaches, managers, board members and cost center heads within the Association is the property of the PA West Soccer Association and may not be given, rented or sold to third parties without the express approval of the Executive Board or its specified representative.

Ownership and Use of Membership Lists
Policy
The membership list of players, coaches, managers, board members and cost center heads within the Association is the property of the PA West Soccer Association and may not be given or sold to third parties without the express approval of the Executive Board or its specified representative.

Intended Use
The Executive Board has the right to determine who may purchase the rights to the PA West Soccer Association membership list, how it may be used, how often it may be used and what financial arrangements may be made. In general, the mailing list will be limited to non-repetitive, soccer related mailings. The material being mailed must be approved by the committee or its representative.

Security of Mailing Lists
To ensure limited access to and utilization of the Association's mailing lists, data will only be sold to bonded entities which will be prohibited from copying or reselling this information. Membership information will not be placed in any literature that would permit open usage for solicitation or resale by private individuals.

Procedure for Sale of Mailing Lists
1. Request for purchase and a copy of the material to be mailed are directed to the Board of Directors or its representative for consideration.
2. Purchaser agrees to terms of sale (limited used, no duplication of list, no resale, etc.).
3. Purchaser provides state office with a copy of content for approval.
4. State office provides data to purchaser upon receipt of good funds.

Cost
Mailing lists may be rented at a cost of .10 per name. The minimum charge 500.00 and the mailing list at this cost will only be provided through a bonded mailing house. Adjustment of the minimum charge is subject to approval of the Executive Board President.

Mailing lists may be rented at a cost of .13 per name, plus postage for mailings handled by the state office. Adjustment of the minimum charge is subject to approval of the Executive Board President.

Presidential Mailing list may be rented for $150.00 through a bonded mailing house.

Guidelines on Anti-Virus Process

Recommended processes to prevent virus problems:

- Always run the Corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in with PA West Soccer's *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Avoid direct media sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan any portal data storage from an unknown source for viruses before using it.
- Back-up critical data and system configurations daily and store the data in a safe place.
- If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
- New viruses are discovered almost every day. Periodically check the *Lab Anti-Virus Policy* and this Recommended Processes list for updates.

Email Policy and Voice Mail Policy

Purpose
To prevent the unauthorized or inadvertent disclosure of sensitive company information.

Scope
This policy covers email forwarding and voice mail, and thereby the potentially inadvertent transmission of sensitive information by all associates, vendors, and agents operating on behalf of PA West Soccer.

Policy
PA West Soccer has provided a facility to enable its customers to communicate with associates of the organization through the use of electronic mail and voice mail. It has also provided a facility whereby associates may communicate with one another through the use of electronic mail and voice mail. All electronic communications and information transmitted by, received by, received from, or stored in these systems are the property of PA West Soccer. Associate use of the network is considered consent to the e-mail and voice mail policy.

3.1 Electronic Mail and Voice Mail
It is the policy of PA West Soccer that its electronic mail system and voice mail system be used only for organization related business and for no other purpose. Associates of the organization shall not use the organization's electronic mail system and/or voice mail system for any other purpose other than the communication of organization business. Customers of the organization shall be discouraged from using the organization's e-mail system and/or voice mail system to communicate with an associate for any purpose other than organization's business. The e-mail system and voice mail system shall not be used to solicit or to advocate any non-company or personal interest. Foul, offensive, defamatory, pornographic or other inappropriate communication is strictly prohibited.

The organization's System Administrator shall monitor all electronic communication through the organization's system to enforce this policy at any time and without prior notice. This will ensure that the system is being used for company purposes only and that our policies on harassment are being followed. All associates must understand that they do not have a personal privacy right in any matter created, received, or sent from the e-mail system and/or voice mail system.

E-mail and voice mail can be read or intercepted by others, including inadvertent disclosure, accidental transmission to third parties, or purposeful retransmission to another associate's internal mailing list. Management should be able to enter an associate's e-mail mailbox or voice mail for business purposes at any time.

It is the policy of PA West Soccer that any communication from a customer received through the organization's electronic mail system and/or voice mail is acted upon with the same and diligence as if the communication had been received in writing. Accordingly, each organization associate who has the capacity of receiving electronic mail and/or voice mail shall check his or her mailbox at least once at the end of the morning and once at the end of each afternoon. Associates should disclose information or messages from the e-mail and/or voice mail network only to authorized associates and managerial staff. E-mail and/or voice mail should be limited to those with a need to know. This applies to both company proprietary information or

confidential material protected by the attorney-client privilege. In some cases, sensitive information should not be sent.

3.3 Messaging
Managers should set policies to ensure that voice and e-mail messages of an associate who are absent and unable to respond to messages for extended periods are reviewed and acted upon in a timely manner. Contingency policies can include use of message forwarding, shard mailboxes and supervisory security overrides, but these are only suggestions.

In the absence of such a policy, managers should implement the following:

When an associate is absent from the organization for one day or longer, it is the responsibility of the associate's supervisor to review any e-mail messages and/or voice mail messages that the associate has received and act upon them appropriately.

It is the policy PA West Soccer that the standard outgoing message for each associate is "You have reached the desk of (associate name). Please leave a message and I will return your call as soon as possible." If the associate is not going to be at work during a business day, the outgoing message should be "This the desk of (associate Name). I will be out of the office until (scheduled return date)."

4.0 Enforcement
Any associate found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

Record Retention

Policy

1. Original copies of invoices, financial statements, bank statements, audit reports, tax forms and contracts shall remain in the State Office.
2. Invoices and vouchers should be retained for five (5) years.
3. Tax records shall be retained for seven (7) years.
4. Employment records should be kept indefinitely but appraisals should only be retained for three (3) years.

Cash Receipts Control

Cash is brought into the State Office. If it is for Coaching or Player Development Programs Amy will process and verify entry form with money and record the receipt; all other items are handled by Cheryl using the same process. Receipt is available to the person paying with cash. Carol completes the deposit in Excel and takes the cash, along with any checks to the bank. Any cash received that is not immediately deposited with be stored in the safe until the next deposit is prepared and taken to the bank.

Cash Disbursement Controls

Initiation of Vouchers:

Any employee or volunteer with responsibility for a particular function may request a voucher for payment of expenses.

Approval of Vouchers:

Each voucher must be approved by a person responsible for the particular Cost Center.

Voucher Verification:

State Office verifies all vouchers are complete and coded to the correct Cost Center.

Check Processing (computerized checks):

Vouchers are entered in the computer by Association Bookkeeper and checks are printed semi-monthly. Dual signatures are required.

Check Processing (manual checks):

Vouchers may be paid by manual check prepared by the Association Bookkeeper. Dual signatures are required for amount more than 500.00.

Check Processing (payroll checks):

Payroll checks are prepared by designated payroll service and approved by the Treasurer. Payroll is distributed via direct deposit to all employees.

Bank Statements:

All bank statements are received at PA West Soccer office.
All bank statements are reconciled by CPA.