Appendix Y: Sample IT Policies and Procedures

Our Pool

Information Technology Policies and Procedures

Developed: July 7, 2008
Revised: January 5, 2009

Our Pool
Information Technology Policies and Procedures

Contents

Our Pool
Information Technology Policies and Procedures

Introduction

Welcome to the Information Technology Policies and Procedures document for Our Pool. Proper use of Information Technology is vital to our ability to provide high quality and high value services to our members.

With this in mind, these policies and procedures have been developed to standardize the approach to the use of Information Technology. More specifically, they are designed to protect such resources as we would other core assets and to maximize the value and usefulness of these assets.

The Information Technology Department or IT Department is available to assist with the implementation and application of these policies and procedures.

Purpose

This technology services policies and procedures manual exists to communicate accepted methods dealing with the use of technology in our organization in a clear and organized manner.

Scope

Unless otherwise stated, these policies apply to all employees, management, contractors, vendors, business partners and any other parties who have access to the technology tools in use at Our Pool.

Non-compliance

Any employee found to have violated these policies may be subject to disciplinary action, up to and including termination of employment. Deliberate violation could include civil and/or criminal prosecution.

Acceptable Use

Purpose

The purpose of Acceptable Use policies and procedures is to inform employees of Our Pool of the rules and procedures that exist for appropriate use of the various technological tools and applications within the organization.

In general, all technological resources owned, leased, licensed or otherwise in use at Our Pool are to be used for business purposes and in a safe and professional manner. Specific lists of acceptable and unacceptable uses exist in individual policies when appropriate.

Ownership and Privacy

All data, messages, files and other content created or stored on our organization's technology resources are the property of Our Pool. Users of our resources cannot expect privacy rights to extend to information stored on or traveling through our systems.

Our Pool reserves the right to inspect all data on any system as a normal course of business.

Outside Parties

Contractors, vendors, business partners and any other parties who have access to the technology tools in use at Our Pool are required to review and acknowledge these policies prior to being provided access the our resources.

Security / Privacy

Data Classification and Disclosure

Public/Unclassified. Information that is generally available to anyone within or outside of the company. Access to this data is unrestricted, may already be available and can be distributed as needed. Examples of Public/Unclassified data are promotional materials, financial audits, agendas, minutes, newsletters and handouts.

Employees may send or communicate a public/unclassified piece of data with anyone inside or outside of the organization.

Private. This is defined as information that is to be kept within the organization. Access to this data may be limited to specific departments and cannot be distributed outside of the workplace. Examples of Private data are claims data and communications related to specific claims.

Employees may not disclose private data to anyone who is not a current employee of the company.

Confidential. This is defined as personal or organization information that may be considered potentially damaging if released and is only accessible to specific groups (HR, WC claims department, etc.) Examples of Confidential data are social security numbers, contact information, communications and other specific claims related data.

Employees may only share confidential data within the department or named distribution list.

Data Protection Compliance

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets requirements for employers and health service providers in the handling of personal and medical related information.
Workers' compensation carriers, including self-insured employers and administrative agencies, are not covered entities under HIPAA. Health-related information being exchanged in conjunction with a workers' compensation claim or appeal is exempted from HIPAA.

SB 1386 & AB 1298

The California Information Practice Act (SB 1386) requires companies that own or have access to personal information of California residents to notify them if their data have (or may have) been accessed illegally.

Personal information this case is defined as an individual's first name or initial and last name in combination with one or more of the following: a social security number, drivers license number (or CA ID number), financial account number and/or credit or debit card information including numbers and passwords, PINs and access codes.

AB 1298 expands the definition of personal information to include medical information and health insurance information such as policy number or subscriber identification number or any information in an individuals application and claims history.

The IT Director will as the sensitive data security and incident coordinator as it relates to this Act. The coordinator should ensure adequate training in the organization as to the extent of the coverage of the Act and what might constitute a breach.

The coordinator will oversee the identification of databases and documents that contain applicable information and ensure adequate controls and security measures are in place.

Suspected breaches should be reported to the coordinator who will conduct an assessment. Based on this assessment, the coordinator, with the concurrence of the appropriate law enforcement representatives (so the investigation might not be impeded) and the Executive Director, will arrange for the communication of the incident to affected individuals, using the communication approach deemed most appropriate.

The coordinator should also review arrangements with third parties who store such data to insure they have adopted equivalent policies and procedures.

Anti-Virus

Any device that may be attached to Our Pool's network(s) must have effective anti-virus protection. This protection must be in working condition and updated with the most current pattern files. All email, incoming and outgoing, will be scanned by the anti-virus application.

Anti-virus protection is managed by the IT Department. Any user that suspects that their anti-virus is not working properly or suspects that they may have contracted a virus on their computer should notify the IT Department immediately.

Software

Any software used for Our Pool business must be appropriately licensed and installed. Any software, including upgrades and downloads, must be installed under the direction of the IT Department.

Removable Media

Removable media includes the following:

- Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives.
- Memory cards in SD, CompactFlash, Memory Stick, or any related flash-based supplemental storage media.
- USB card readers that allow connectivity to a PC.

- Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function.
- PDAs, cell phone handsets, and smartphones with internal flash or hard drive-based memory that support a data storage function.
- Digital cameras with internal or external memory support.
- Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks.
- Any hardware that provides connectivity to USB devices through means such as wireless (WiFi, WiMAX, irDA, Bluetooth, among others) or wired network access.

The policy applies to any hardware and related software that could be used to access corporate resources, even if said equipment is not corporately sanctioned, owned, or supplied.

The overriding goal of this policy is to protect the integrity of the private and confidential data that resides within Our Pool's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently moved outside the enterprise network and/or the physical premises where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to our organization's public image. Therefore, all users employing removable media and/or USB-based technology to backup, store, and otherwise access data of any type must adhere to these processes for doing so.

Threats

Some of the threats that exist from the use removable media are:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive corporate data is deliberately stolen and sold by an employee.
Copyright	Software copied onto portable memory device could violate licensing.
Spyware	Spyware or tracking code enters the network via memory media.
Malware	Viruses, Trojans, Worms, and other threats could be introduced via external media.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the enterprise to the risk of non-compliance with various identity theft and privacy laws.

Addition of new hardware, software, and/or related components to provide additional USB-related connectivity within corporate facilities will be managed at the sole discretion of IT. Non-sanctioned use of USB-based hardware, software, and/or related components to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

Affected Technology

All USB-based devices and the USB ports used to access workstations and other related connectivity points within the corporate firewall will be centrally managed by Our Pool's IT department and will utilize encryption and strong authentication measures. Although IT is not able to manage the external devices – such as home PCs – to which these memory resources will also be connected, end users are expected to adhere to the same security protocols when connected to non-corporate equipment.

It is the responsibility of any employee who is connecting a USB-based memory device to the organizational network to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. Based on this, the following rules must be observed:

Access Control

1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect removable media and USB devices to our network infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts systems, data, users, or members at risk.

2. Prior to initial use on the network or related infrastructure, all USB-related hardware and related software must be registered with IT. A list of approved USB devices and related software is available from IT.

Security

3. Employees using removable media and USB-related devices and related software for data storage, back up, transfer, or any other action within Our Pool's technology infrastructure will, without exception, use secure data management procedures. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

4. All USB-based devices that are used for business interests must be pre-approved by IT, and must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data. Any outside computers used to synchronize with these devices will have installed whatever anti-virus and anti-malware software deemed necessary by our IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be used must be updated in accordance with existing company policy.

5. All removable media will be subject to quarantine upon return to the office before they can be fully utilized on enterprise infrastructure.

6. Passwords and other confidential data as defined by our IT department are not to be stored on portable storage devices.

7. Any USB-based memory device that is being used to store our data must adhere to the authentication requirements of our IT department. In addition,

all hardware security configurations (personal or company-owned) must be pre-approved by our IT department before any data-carrying memory can be connected to it.

8. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once their use is no longer required.

9. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of our IT department. This includes, but is not limited to, reconfiguration of USB ports.

10. IT may restrict the use of Universal Plug and Play on any client PCs that it deems to be particularly sensitive. IT also reserves the right to disable this feature on PCs used by employees in specific roles.

11. IT reserves the right to summarily ban the use of these devices at any time. IT need not provide a reason for doing so, as protection of confidential data is the highest and only priority.

12. IT reserves the right to physically disable USB ports to limit physical and virtual access.

13. IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the network.

14. Users agrees to immediately report to his/her manager and our IT department any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.

Hardware Disposal

To protect software license agreements and the confidentiality of personal information Our Pool has a policy of pre-disposal hardware sanitation.

This applies to all hardware that will be transferred externally including that which is:

- Transferred to the private ownership of employees
- Donated to charitable organizations
- Returned to vendor for servicing or maintenance
- Released to an external agency for disposal

This applies to all hardware that is being retired or disposed including servers, workstations, PDA's and cell phones and removable storage media.

Servers, PCs and notebooks – Hard drives must be "wiped" using a process meeting U.S. Department of Defense specifications or destroyed. For computers where operating systems or applications will be donated or transferred with the system, the hard drive must still be wiped. The applications may be re-installed after wiping and reformatting.

Other devices such as PDA and cell phones must be wiped of data and reset to factory settings. They may also be destroyed prior to disposal.

Removable storage such as flash memory devices, CD and DVD media, tape or other storage media should be destroyed prior to disposal.

Physical

Physical security is an important facet of any system security plan. Physical access must be regulated and an acceptable environment must be maintained as follows:

Server, Router and Wiring Closet

1. Servers, routers and the wiring closet will be located in a secure location in which access can be limited to those employees approved by the IT Manager or the Executive Director.

2. Non-employees that have been approved by the IT Manager or the Executive Director (e.g. technicians) will be accompanied by an approved IT employee while they have access to the servers.

3. Power backup systems should be in place and adequate for 10 minutes of operation during a power loss. Servers should be configured for auto shutdown if power loss is longer than 5 minutes.

4. A fire extinguisher designed for use with electronics (e.g. a carbon dioxide-based unit) will be present and visible in these locations.

5. All equipment will be either solidly on the floor, installed in secured racks or secured to a wall.

6. All units will be stored in an area of adequate environmental controls including temperature not greater than 78 degrees F. Adequate ventilation and/or fans will be provided to help dissipate heat around units including power supplies.

Workstations and Printers

7. All workstations will be connected to power through an uninterruptible power supply – preferably to one that provides power conditioning or, at the least, power surge protection.

Printers and Copiers

8. All printers and copiers will be connected to power through a surge protector.

9. Print and copy jobs should be picked up immediately upon completion. Printed and copied jobs containing non-public information should be observed and removed by the appropriate employee.

The IT Manager will conduct an audit at least annually to insure that this policy is being adequately met.

Passwords

Passwords are an important component of our security systems. Passwords are used to authenticate any user which can then dictate what systems and information they are authorized to access.

Therefore, passwords must be created, used and protected appropriately to insure that our security requirements are being met.

Password Construction and Modification

1. Passwords must be a minimum of 8 characters in length, and use at least 3 of 4 character types (lower case letters, uppercase letters, numbers and special characters.)

2. For general applications such as workstation login, passwords must be changed annually.

3. For confidential or private data or applications vulnerable to fraud (such as the claims processing program or the accounting system), passwords must be changed quarterly.

Password Protection

4. Passwords are to be treated as confidential information. Under no circumstances is an employee to give, tell, or hint at their password to another person, including IT staff, administrators, superiors, other co-workers, friends, and family members.

5. Under no circumstances will any member of the organization request a password without the request coming from both a representative of the IT department and the user's direct manager. Should a request be made that does not conform to this standard, immediately inform both the IT department and your direct manager.

6. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to company resources via the company's Virtual Private Network or SSL-protected Web site.

7. No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form.

8. Do not use the "Remember Password" feature of applications.

9. Passwords used to gain access to company systems are not to be used as passwords to access non-company accounts or information. Similarly, passwords used to access personal, non-work related accounts are not to be used to access company accounts.

10. Each application, system and data point should be protected by a different password where possible. The use of the same password to protect all access is strongly discouraged.

11. If an employee either knows or suspects that his/her password has been compromised, it must be reported to the IT Department and the password changed immediately. If the minimum aging requirement has not been met for the password, the IT department will reset the minimum aging for the account allowing the user to create a new password.

12. The IT Department may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

Disaster Planning

It is Our Pool's policy to have a current Disaster Recovery Plan (DRP) process in place.

For Our Pool, the IT Director serves as the DRP coordinator.

The coordinator is responsible for overseeing the development and maintenance of the DRP. All departments and job functions must be included in these activities.

The plan will be reviewed and tested annually.

Though the plan is developed and maintained through the IT Department, Executive Management and, in particular, the Executive Director is ultimately responsible for the quality and applicability of the plan.

Though information technology policies and procedures are a significant part of disaster planning and business continuity, it is beyond the scope of this document. Please refer to Our Pool's Disaster Recovery Plan.

Backup and Recovery

This section focuses on the day-to-day operational need for backup and recovery.

Data Backup and Recovery

Local Systems Backup

The local systems backup policy governs how and when data residing at Our Pool's facility will be backed up and stored for the purpose of providing restoration capability. In addition, it addresses methods for requesting that backed up data be restored.

What Is Backed Up

Some programs and all data that reside on Our Pool's servers are backed up nightly to portable removable storage devices.
Data that reside on individual PCs, workstations or notebooks are not backed up. Data should not be stored on these devices except temporarily or as required due to circumstances. End users are strongly encouraged to save their data to the appropriate server so that their data is backed up regularly in accordance with this policy.
In addition, files that are left open at the time the backup procedure is initiated may not be backed up. End users should save and close all files, as well as all related applications, prior to the backup procedure window.
It is the responsibility of server administrators to ensure that all new servers be added to the backup routine. Prior to deploying a new server, a full backup must be performed and the ability to perform a full restoration from that backup confirmed. Prior to retiring a server, a full backup must be performed and placed in permanent storage.

Backup Schedule

Backups are conducted automatically nightly Monday through Friday. All servers will be backed up according to the following procedure. This method ensures that no more than one day's working data will be missing in the event of a data loss incident:

1. All backup drives are to be labeled with the day(s) of the week they are to be used and a number. The combination of the two should create a unique identifier for that drive.

2. Backup drives stored on site will be stored in a locked cabinet stored beyond the immediate vicinity of the servers.

3. Backup drives stored off-site are to be stored in a secure location acceptable to the IT Director and the Executive Director

4. All backups will take place between the hours of 12 a.m. and 6 a.m. This timeframe has been selected to minimize the impact of server downtime on end users that may be caused by the need to take servers or databases offline in order to perform the backup itself. If this backup schedule in some way interferes with a critical work process, then the affected user(s) is to

notify the IT Department so that exceptions or alternative arrangements can be made.

5. A full backup will be performed daily, Monday through Thursday. The backup drive will be stored during the day then re-attached to the server at the end of the day. The drive will be taken off-site at the end of the day Friday then returned to the office on Monday.

6. A full backup will be performed each Friday. This drive will be stored off-site and returned to the office on Friday. It will be attached to the drive at the end of the day Friday and removed off-site again on Monday.

7. A full backup will be performed at the end of each month. This drive will be removed to a 2nd site under the auspices of the IT Director. It will be returned monthly and only to make the monthly backup. A minimum of 12 months of backups should be stored in this manner with as many drives as required to do so.

8. A full backup will be performed annually. This drive will be removed to a 3rd site under the auspices of the IT Director. Backups for three years should be maintained in the manner.

9. All server backups performed must be noted in the server backup log immediately upon completion. All server backup log sheets must be kept in an appropriately labeled three-ring binder in an agreed-upon, centralized location. The log must include the date of backup, hard drive used and initials of the administrator managing that day's backup.

Managing Restores

The ultimate goal of any backup process is to ensure that a restorable copy of data exists. If the data cannot be restored, then the process is useless. As a result, it's essential to regularly test one's ability to restore data from its storage media.

1. All daily backup drives must be tested at least once every month to ensure that the data they contain can be completely restored.

2. All weekly tapes must be tested at least once every 6 months to ensure that the data they contain can be completely restored.

3. All monthly tapes must be tested at least once every [insert number] years to ensure that the data they contain can be completely restored.

Users requesting a restore should provide the following information to the IT Department:

1. Reason for the requested restore (e.g. accidental deletion, corrupted file, accidental overwrite)

2. Name of file(s) or folder(s) to be restored and their location or, in the case of deletion, their last known location.

3. Level of importance and urgency

The IT Department member responsible for overseeing backup and restore procedures will develop a restore plan based on the extent of the data loss and which backup medium will likely need to be accessed. The IT person will then discuss the plan with the user and so they can agree on an acceptable time frame.

Workstation and Notebook Backup

Original workstation and notebook program install and recovery media should be stored in a secure location accessible to the IT Department. No non-temporary/non-reproducible data should be stored on individual workstations or notebooks.

Therefore, there is no reason for workstations or notebooks to be backed up.

Backup of Off-site Data

Much of Our Pool's most critical data is stored remotely as part of hosted applications. Though these applications and related data is maintained by a third party, the data belongs to Our Pool and it is our responsibility to make sure the data is protected.

The following must be considered as they relate to data stored off-site:
Third party hosts of Our Pool data must be held to documented standards based on the importance of the specific system and data as follows.

Claims Application

Annually: Vendor must show proof of a comprehensive security approach. Mirrored co-location is a requirement. A documented Disaster Recovery Plan must be available for viewing by our representative. Adequate system and support including hacking and virus prevention must be demonstrated.

Web site (static)

The static and public portion of Our Pool's Website should be hosted on service with demonstrated down time prevention processes including anti-hacking and anti-virus. (Note: the site should be backed up periodically (e.g. monthly) to Our Pool's servers.

Web site (database)

The member's only database-based portion of Our Pool's Website host must demonstrate daily backup with restore service guarantees and include anti-hacking and anti-virus protection and monitoring.

Systems

A system for the purposes of this section refers to individual or combined hardware or components that make up the whole of organizational technology. This can include individual workstations, servers, routers, switches, printers, battery backup systems, etc.

All systems used in Our Pool should have a readily identifiable source for repair or replacement. The IT Department is responsible for maintaining an inventory of systems and availability required of each system. The IT Department must then have a process by which each system can be repaired or replaced within the parameters of the availability requirements.

Email and Messaging

Email is critical for business communication at Our Pool. Messaging, including texting and Instant Messaging, may also be valuable for some communication scenarios. Therefore, email and texting should be used in a manner consistent with other essential business communication methods.

General Expectations

Employees are expected to check their email in a consistent and timely manner. If they are not available to do so, they should set up an auto-reply so that those attempting to communicate with them in this manner will know when they should expect a reply or how they should proceed if the item is more pressing.

Users are responsible for mailbox management including organization and cleaning. They are also responsible for managing those emails marked as spam by any one of our spam filters.

Users are expected to remember that any electronic communication sent from Our Pool reflects on our organization and even our members. All such communication should comply with normal standards of professional and personal courtesy and conduct.

Appropriate Use

Individuals are encouraged to use e-mail and messaging to further the goals and objectives of our organization. The types of activities that are encouraged include:

1. Communicating with fellow employees, business partners of Our Pool, and clients within the context of an individual's assigned responsibilities.

2. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.

3. Participating in educational or professional development activities.

Inappropriate Use

Our e-mail systems and services are not to be used for purposes that could be reasonably expected to strain storage or bandwidth (e.g. e-mailing large attachments instead of pointing to a location on a shared drive). Individual e-mail use will not interfere with others' use of our e-mail system and services. E-mail use must comply with all applicable laws and all organizational policies.

The following activities are deemed inappropriate uses of our email and messaging systems and services and are prohibited:

1. Use of e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).

2. Use of e-mail in any way that violates Our Pool's policies, rules, or administrative orders.

3. Viewing, copying, altering, or deletion of e-mail accounts or files belonging to our organization or another individual without authorized permission.

4. Sending of unreasonably large e-mail attachments.

5. Opening e-mail attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.

6. Sharing e-mail account passwords with another person, or attempting to obtain another person's e-mail account password. E-mail accounts are only to be used by the registered user.

7. Excessive personal use of Our Pool's e-mail resources. Our Pool allows limited personal use for communication with family and friends, independent learning, and community service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources. Our Pool prohibits personal use of its e-mail systems and services for unsolicited mass mailings, commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.

Monitoring and Confidentiality

The e-mail systems and services used at Our Pool are owned by the organization, and are, therefore, its property. This gives Our Pool the right to monitor any and all e-mail traffic passing through its e-mail system. This monitoring may include, but is not limited to, inadvertent reading by IT staff during the normal course of managing the e-mail system, review by the legal team during the e-mail discovery phase of litigation, observation by management in cases of suspected abuse or to monitor employee efficiency.

In addition, archival and backup copies of e-mail messages may exist, despite end-user deletion, in compliance with our records retention policy. The goals of these backup and archiving procedures are to ensure system reliability, prevent business data loss, meet regulatory and litigation needs, and to provide business intelligence. Backup copies exist primarily to restore service in case of failure. Archival copies are designed for quick and accurate access for a variety of management and legal needs. Both backups and archives are governed by our document retention policies.

If Our Pool discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, e-mail records may be retrieved and used to document the activity in accordance with due process. All reasonable efforts will be made to notify an employee if his or her e-mail records are to be reviewed. Notification may not be possible, however, if the employee cannot be contacted, as in the case of employee absence due to vacation.

Use extreme caution when communicating confidential or sensitive information via e-mail. Keep in mind that all e-mail messages sent outside of our organization become the property of the receiver. A good rule is to not communicate anything that you wouldn't feel comfortable being made public. Demonstrate particular care when using the "Reply" command during e-mail correspondence to ensure the resulting message is not delivered to unintended recipients.

Remote Computing

Remote Access

Purpose and Scope

Any and all work performed for Our Pool on said computers by any and all employees, through a remote access connection of any kind is covered by the following policy. Work can include but is not limited to email, Web browsing, intranet resources and any other company application used over a remote connection. Remote access is defined as any connection to Our Pool's network and/or other company sponsored applications from off-site locations such as employee homes, hotel rooms, airports, café's, satellite offices, wireless devices, etc.

All remote access will be centrally managed by Our Pool's IT department and will utilize encryption and strong authentication measures. External devices used must meet a minimum requirement for performance, security and safety as decided by the IT department. Those who do not meet these requirements may be denied remote access privileges.

Employees, contractors or other agents requiring the use of remote access for business purposes must be approved by the IT department and Executive Management. The reason for the need for remote access including the extent of system access and level of service should be submitted in writing and approved by Executive Management prior to the IT department providing such access.

Appropriate Use

It is the responsibility of any employee of [company name] with remote access privileges to ensure that their remote access connection remains as secure as his or her network access within the office. It is imperative that any remote access connection used to conduct [company name] business be utilized appropriately, responsibly, and ethically. Therefore, the following rules must be observed:

1. Employees will use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with Our Pool's password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

2. All remote computer equipment and devices used for business interests, whether personal- or company-owned, must display reasonable physical security measures. Computers will have installed whatever antivirus software deemed necessary by Our Pool's IT department.

3. Remote users using public hotspots for wireless Internet access must employ for their devices a company-approved personal firewall, VPN, and any other security measure deemed necessary by the IT department. VPNs supplied by the wireless service provider should also be used, but only in conjunction with Our Pool's additional security measures.

4. Hotspot and remote users must disconnect wireless cards when not in use in order to mitigate attacks by hackers, eavesdroppers and other outsiders.

5. All hardware security configurations (personal or company-owned) must be approved by Our Pool's IT department.

6. Employees, contractors, and temporary staff will make no modifications of any kind to the remote access connection without the express approval of Our Pool's IT department. This includes, but is not limited to, split tunneling, and any non-standard hardware or security configurations, etc.

7. Employees, contractors, and temporary staff with remote access privileges must ensure that their computers are not connected to any other network while connected to Our Pool's network via remote access, with the exception of Internet connectivity.

8. In order to avoid confusing official company business with personal communications, employees, contractors, and temporary staff with remote access privileges must never use non-company e-mail accounts (eg. Hotmail, Yahoo, etc.) to conduct Our Pool's business.

9. No employee is to use Internet access through company networks via remote connection for the purpose of illegal transactions, harassment, competitor interests, or obscene behavior, in accordance with other existing employee policies.

10. All remote access connections must include a "time-out" system. In accordance with Our Pool's security policies, remote access sessions will time out after a set time of inactivity. Time-outs will require the user to reconnect and re-authenticate in order to re-enter company networks.

11. If a personally- or company-owned computer or related equipment used for remote access is damaged, lost, or stolen, the authorized user will be responsible for notifying their manager and Our Pool's IT department immediately.

12. The remote access user also agrees to immediately report to their manager and Our Pool's IT department any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.

13. The remote access user also agrees to and accepts that his or her access and/or connection to Our Pool's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

Mobile Computing

Mobile devices are important to the efficiency and productivity of Our Pool. However, since they are most often used outside of the local office environment, they represent a significant risk both in data security and risk of damage and theft.

E-Data Retention

(Under Construction)

Working files

Imaged and read only e-files

Email, voicemail and phone messages

Telephones and Cellular devices

Telephone communication is an essential part of the day-to-day operations of Our Pool. Telephone and voicemail services are provided to employees to facilitate performance of Our Pool's work.

Basic Policy

The use of telephones and voicemail should be as cost effectively as possible and in keeping with the best interests of Our Pool. All employees must operate within the following basic policy guidelines. Further information on appropriate and inappropriate use follows this section.

1. All telephones, telephony equipment, voicemail boxes, and messages contained within voicemail boxes are the property of Our Pool.

2. The number of telephone calls made should be limited in number and duration to that necessary for effective conduct of business.

3. All voicemail boxes will be protected with a PIN (personal identification number). PINs must not be shared with others.

4. A voicemail box can hold 30 minutes of message storage time. If a voicemail box is full, no further messages can be recorded. Read voicemail messages will be automatically deleted after 30 days.

5. Voicemail is to be used as a backup in the event you are not available to answer a call, and should not be used to "screen" calls. Each user is expected to respond to voicemail messages in a timely manner.

6. If you will be away from the office for more than one business day, you are expected to change your voicemail greeting to reflect this fact and direct callers to alternate contacts if applicable.

7. Use of directory assistance (i.e. 411) should be avoided since a fee is incurred with each use. If you are unsure of a number, please consult print or online telephone directories first.

Unacceptable Use

Our Pool telephone and voicemail services may not be used for the following:

1. Transmitting obscene, profane, or offensive messages.

2. Transmitting messages or jokes that violate our harassment policy or create an intimidating or hostile work environment.

3. Using the telephone system or breaking into a voicemail box via unauthorized used of a PIN or other password.

4. Broadcasting unsolicited personal views on social, political, or other non-business related matters.

5. Soliciting to buy or sell goods or services unrelated to Our Pool.

6. Calling 1-900 phone numbers.

7. Making personal long-distance phone calls without supervisor permission.

Limited Personal Acceptable Use

In general, personal use of telephone and voicemail services is allowable, but must be limited in number and duration and must not interfere with performance of official business duties. Limited personal acceptable use is allowed under the following circumstances:

1. An employee's work schedule changes without advance notice and the employee must notify a family member or make alternate transportation or childcare arrangements.

2. Brief local calls to a spouse, minor child, or elderly parent, or to those responsible for them (e.g. school, daycare center, nursing home).

3. The employee needs to make a call that can only be made during regular working hours, such as to a doctor or local government agency.

4. The employee needs to make arrangements for emergency repairs to his or her residence or automobile.

5. A call that reasonably could not be made at another time and is of moderate duration.

Monitoring

Our Pool reserves the right to monitor telephone and voicemail use, including telephone conversations and the contents of voicemail boxes. Monitoring of telephone and voicemail use will only be done for legitimate reasons, such as to assess customer service quality assurance, retrieve lost messages, recover from system failure, or comply with investigations of wrongful acts.

Internet Usage

Purpose

The goal of this policy are to outline appropriate and inappropriate use of Our Pool's Internet resources, including the use of browsers, electronic mail and instant messaging, file uploads and downloads, and voice communications.

Internet access is controlled through individual accounts and passwords. Department managers are responsible for defining appropriate Internet access levels for the people in their department.

Appropriate Use

Individuals are encouraged to use the Internet to further the goals and objectives of Our Pool. The types of activities that are encouraged include:

1. Communicating with fellow employees, business partners and members within the context of an individual's assigned responsibilities;

2. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities; and

3. Participating in educational or professional development activities.

Inappropriate Use

Individual Internet use shall not interfere with others' productive use of Internet resources. Users will not violate the network policies of any network accessed through their account. Internet use at Our Pool will comply with all Federal and State laws, all organizational policies, and all contracts. This includes, but is not limited to, the following:

1. The Internet may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).

2. The Internet may not be used in any way that violates our organization's policies, rules, or administrative orders. Use of the Internet in a manner that is not consistent with the mission of our Pool, misrepresents Our Pool, or violates any organizational policy is prohibited.

3. Individuals should limit their personal use of the Internet. Our Pool allows limited personal use for communication with family and friends, independent learning, and community service. We prohibits use for mass unsolicited mailings, access for non-employees to Our Pool's resources or network facilities, uploading and downloading of files for personal use, access to pornographic sites, gaming, un-related commercial activity, and the dissemination of chain letters.

4. Individuals may not establish company computers as participants in any peer-to-peer network, unless approved by management.

5. Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to Our Company or another individual without authorized permission.

6. In the interest of maintaining network performance, users should not send unreasonably large electronic mail attachments or video files not needed for business purposes.

7. Individuals will only use organization-approved services for voice communication over the Internet.

Blogs, Instant Messaging, Facebook, Twitter, and related

(Under Construction)

Security

For security purposes, users may not share account or password information with another person. Internet accounts are to be used only by the assigned user of the account for authorized purposes. Attempting to obtain another user's account password is strictly prohibited. A user must contact the IT department to obtain a password reset if they have reason to believe that any unauthorized person has learned their password. Users must take all necessary precautions to prevent unauthorized access to Internet services.

Monitoring and Filtering

Our Pool may monitor any Internet activity occurring on its equipment or accounts. We may employ filtering software to limit access to sites on the Internet. If we discover activities which do not comply with applicable law or departmental policy, records retrieved may be used to document the wrongful content in accordance with due process.

Disclaimer

Our Pool assumes no liability for any direct or indirect damages arising from the user's connection to the Internet. We are not responsible for the accuracy of information found on the Internet and only facilitate the accessing and dissemination of information through its systems. Users are solely responsible for any material that they access and disseminate through the Internet.