Arizona Department of Veterans' Services

Information Technology Packet

ARIZONA DEPARTMENT OF VETERANS' SERVICES

INTERNAL MANAGEMENT POLICY 00-02

SUBJECT: INTERNET USAGE

EFFECTIVE DATE: April 8, 2010 (Supersedes September 18, 2003)

1.0 POLICY: It is the policy of the Arizona Department of Veterans' Services (ADVS) to provide employees with Internet access and guidance on its use. The Internet is a communications tool made available to selected ADVS employees to enhance performance of their duties. Its use should be managed by rules of conduct applicable to any other Information Technology (IT) resource.

2.0 AUTHORITY: A.R.S. § 41-604, Duties and powers of the (ADVS) director; § 41-3504.A.1.(13), Powers and duties of the (GITA) agency; violation; classification; and § 41-1350, Records definition.

3.0 RESPONSIBILITY: Internet users shall comply with all applicable federal and state laws, including A.R.S. § 38-448, ADVS policies, procedures and guidelines. The IT Section is responsible for providing education on Internet use and giving employees acknowledgement forms to be signed. Supervisors are responsible for notifying the IT Section when employees require Internet access and collecting signed acknowledgement forms from employees. The ADVS Human Resources Section is responsible for filing acknowledgements in the official personnel file. Violation of this policy may result in revocation of the privilege to access the Internet and/or disciplinary action.

4.0 DEFINITIONS:

4.0 "Information Technology (IT)" means all computerized and auxiliary automated information processing, telecommunications and related technology, including hardware, software, vendor support and related services, equipment and projects.

4.1 "IT Section" means the ADVS office responsible for all aspects of IT for the agency (including Internet access for the agency).

4.2 "Human Resources Section" means the ADVS office responsible for all aspects of Human Resource issues for the agency.

4.3 "Internet" means an electronic communications network that connects computer networks and organizational computer facilities around the world.

4.4 "Internet user" means an agency employee, contract employee or other agency-authorized person who accesses the Internet through the use of state/agency owned/controlled computer equipment.

5.0 PROCEDURES:

5.0 Internet access is an IT/computer service and is the property of ADVS and the State of Arizona. ADVS reserves the right to monitor Internet use by any user at any time. The ADVS director or IT manager may determine

appropriate use and deny, revoke, suspend or close any user account at any time, based upon a determination of inappropriate use.

5.1 Employees who have a personal computer at their work site may, with appropriate supervisory permission, have access to the Internet. Access is primarily intended as a business tool for conducting authorized state activities. Examples of business related Internet use include, but are not limited to:

5.1.1 Communications and information exchanges directly relating mission, goals and work tasks of ADVS.
5.1.2 Announcements of state laws, procedures, hearings, policies, services or activities.
5.1.3 Use for advisory, standards, research, analysis, and professional society or development activities related to the user's departmental duties and responsibilities.
5.1.4 Ordering products through a business web site in accordance with procurement procedures.

5.2 ADVS believes appropriate use of the Internet can enhance the quality of an employee's work experience and is conducive to increased productivity while at work. ADVS encourages employees to make judicious use of this unique tool and recognizes employees may need to access the web for personal business, similar to using the telephone. ADVS expects employees to be engaged in work-related tasks during their assigned duty hours. Private use of the Internet only should occur during breaks, lunch periods or off-duty periods before or after work. Some examples of acceptable private use include, but are not limited to:

5.2.1 Increasing knowledge of, and familiarity with, the Internet through use and practice.
5.2.2 Conducting business with government entities such as registering an automobile with the Motor Vehicle Division of the Arizona Department of Transportation.
5.2.3 Maintaining contact with business organizations such as news bureaus or organizations.
5.2.4 Research and study.
5.2.5 Using e-mail to maintain personal correspondence.

5.2.5.1 Personnel should not use the ADVS internal E-mail system for personal use. If a user wishes to send personal correspondence, Internet based E-mail systems such as Hotmail, Yahoo and the like should be utilized instead.
5.2.5.2 Internet E-mail is subject to the same restrictions and guidelines contained in the ADVS E-mail Usage IMP 00-01.
5.2.5.3 Users should not consider E-mail to be either private or secure.
5.2.5.4 E-mail via the Internet is not as reliable or as secure as

internal E-mail.

5.2.5.5 Internet E-mail users should be aware that ADVS monitors Internet use, including sites visited, without user consent and without prior notice.

5.2.5.6 Employees wishing to check personal E-mail accounts (e.g., Hotmail, Yahoo, or web mail from their ISP [Internet Service Provider]) using ADVS equipment should think about the content of any E-mail in their personal accounts prior to accessing it. If any content includes rude or offensive language, nudity or depictions of nudity, or sexual content, it should not be accessed.

5.2.6 The use of Streaming Audio or Video such as Real Player or Windows Media Player for personal use is prohibited. Streaming Audio and Video tends to slow down Internet connection for the site as well as slow response times on network applications.

5.3 It is unacceptable for an Internet user to view, submit, publish, display, or transmit on the network, or any ADVS computer system, any information that:

5.3.1 Violates or infringes on the rights of any other person.

5.3.2 Contains defamatory, false, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material.

5.3.3 Contains rude or offensive language, nudity or depictions of nudity, or any type of sexual content, or ultimate sex acts (as defined in Title 38, ARS § 38-448).

5.3.4 Violates any applicable federal, state or agency regulations prohibiting sexual harassment.

5.3.5 Intentionally restricts or inhibits other authorized users from using the system or the efficiency of the computer systems.

5.3.6 Encourages the use of controlled substances or uses the system for the purpose of criminal intent.

5.3.7 Uses the system for any other illegal purpose.

5.3.8 Solicit any activity prohibited by law.

5.3.9 Transmit material, information, or software in violation of any local, state, or federal law.

5.3.10 Conduct any political activity.

5.3.11 Conduct any gambling, betting or gaming activity.

5.3.12 Conduct any activity for personal gain (e.g., stock trading).

5.3.13 Make unauthorized purchases.

5.4 Consent – All Internet users shall acknowledge and consent that all Internet, network and Information Systems activity is the property of ADVS and the State of Arizona, and therefore, should not consider any Internet activity to be private.

5.4.1 The IT Section is authorized to monitor all Internet traffic and to use tracking software, or other state agencies/independent contractors

for the purpose of monitoring Internet traffic. Any violations will be reported to the appropriate supervisor for disciplinary action.

5.4.1.1 IT Section personnel are authorized to view material deemed unauthorized in section 5.3 of this policy for the purposes of monitoring and verification.

5.4.2 The IT Section understands accidents can happen. If there is a situation where an employee accidentally clicks on an Internet link that brings up an inappropriate website, the employee should immediately report in writing to his/her supervisor the situation including the name of the site viewed and time of access.

5.5 Social Networking and related sites

5.5.1 Proper usage of Social Networking

5.5.1.1 State personnel and contractors in a budget unit who are responsible for content in social networking efforts shall first obtain approvals from the Budget unit CEO and CIO before registering and participating on behalf the State. State personnel, including but not limited to volunteers, students, interns and other representatives working with the state or an agency ("Personnel"), contractors, and vendors with a personal social networking registration or license shall not use a personal social network, web blog or blog system for conducting state business.

5.5.1.2 Budget unit CIO's shall develop and maintain a Social Networking Matrix that identifies state personnel and contractors participating in social networking activities which shall include the social networking application name (i.e., MySpace, Twitter, Facebook, Nixle.com, etc.), first and last name of the individual, username (if applicable), email address, and password. Password information may be maintained in any auditable and retrievable format depending on agency policy, standards and procedures.

5.5.1.3 Upon termination of personnel or contractors, the budget unit CIO shall be responsible for removing/deleting social networking registrations of such state personnel and contractors within 30 days or less of termination or contract expiration.(P800-S810 Rev 2.0 § 4.4.3)

5.5.1.4 GITA reserves the right to request a copy of a Budget units' Social Networking Matrix to address data/information risks, privacy issues, and security vulnerabilities/assurances for the state and for the Department of Homeland Security. TISA will be modified for agencies to electronically submit their Social Networking Matrix by FY2011 when submitting annual TISA compliance reports.

5.5.1.5 Jurisdiction and authority for the retention of public records remains with the State Library of Archives and Public Records (ASLAPR). The issue of public records for state programs and services should be addressed by each state agency with ASLAPR for compliance by the very nature of its content and whether it serves the state and/or the public.

5.5.2 Social Networking Activities

5.5.2.1 All social networking activities shall address programs and services of the business unit in support of its mission and delivery of services.

5.5.2.2 Before participating in any online activities, understand that anything posted online through social networking is available to anyone in the world. Any text or photo placed online is completely out of your control the moment it is placed online – even if you limit access to your site.

5.5.2.3 State personnel/contractors shall not post information, photos, links/URLs or other items online that would reflect negatively on any individual(s), its citizens, or the state, unless approved by agency policy.

5.5.2.4 State personnel/contactors shall not provide any confidential information pertaining to the State and home addresses, personnel phone number(s), birth date, or any other personal identifying information, as well as personal location or personal plans on a web blog or other social network system. By doing so, personal information could contribute to identity theft, personal harm and/or loss of property.

5.5.2.5 Budget unit web blogs/media shall have clear disclaimers that their views represent the best interest of state and its citizens. All web blogs shall be clear, direct, professional, honest, ethical, and written in the first person.

5.5.2.6 Be respectful and mindful of the state, in addition to state leadership, state employees, customers, partners, vendors, citizens, and the public when participating in social networks and web blogs.

5.5.2.7 A budget unit's online presence reflects a perception of the State. Be aware that images and comments reflect views and directions of the State, whether real or perceived.

5.5.2.8 State Personnel/contractors shall not reference, cite, or publish information, views or ideas of any third party without their written consent and only as permitted by the State for the purpose of conducting business on behalf of the State.

5.5.3 Security and Privacy

5.5.3.1 State web blogs shall comply with the security and

privacy policies/standards of the State (EO 2008-10). This applies to comments provided on other blogs, forums, and other social networking sites on behalf of the state. Information posted to the state web blog or external blogs or other social network sites is a public record. Personal identifying information, other confidential information or sensitive information is not permitted for posting to a blog or social network site.

5.5.3.2 Each agency is responsible for reporting and responding to information security and privacy incidents, including breach notification requirements, if personal identifying information or other confidential or sensitive information is posted to a web blog or other social network system.

5.5.3.3 Under no circumstance should State authorized business that involves the communication of personal identifying, confidential or sensitive information be conducted on a social network, web blog or blog system.

5.6 Copyright laws must be obeyed. All communications and information accessible via the Internet should be assumed to be private property. Internet users shall honor copyright laws, including those protecting software and intellectual property.

5.6.1 Duplicating, transmitting, or using software not in compliance with software license agreements is considered copyright infringement.

5.6.2 Users shall not make copies of software or literature without proper authorization and the full legal right to do so.

5.6.3 Unauthorized use of copyrighted materials, or another person's original writings, is considered copyright infringement.

5.6.4 Internet users shall not transmit copyrighted materials, belonging to others, over the Internet without permission.

5.6.5 If ADVS permits, users may download copyrighted material from the Internet, but its use must conform to the restrictions posted by the author or current copyright law.

5.6.6 Copyrighted information used on web sites must be clearly identified as such.

5.6.7 Public domain material may be downloaded for business related use. Redistribution of public domain materials is done so with the assumption of all risks regarding the determination of whether or not the materials are in the public domain. Any redistribution of public domain materials is strictly limited to non-commercial use.

5.6.8 The use of peer-to-peer file sharing applications such as Kazaa, Morpheus, iMESH and similar programs is strictly prohibited.

5.7 Downloading – Downloading information from the Internet is permitted only when it meets the restrictions of the ADVS director or IT Manager.

5.7.1 If a user's downloaded material may have been infected by a virus, the user should contact the IT Section immediately.

5.7.2 The use of screensaver programs, mouse pointer programs, and

other desktop enhancing software is not allowed. These programs may allow for additional backgrounds, screensavers, cursors, etc., but they can affect the performance of the computer. Examples of this software include Webshots, Comet Cursor, Bonzi Buddy, etc. If an IT Section staff member deems any of the downloaded software to be adversely affecting the performance of the PC, the IT Section staff member shall be authorized to remove the software and immediately notify the employee's supervisor. Once removed, the software is prohibited from re-installation. If the employee re-installs the software, the IT Section shall inform the employee's supervisor for disciplinary action.

5.7.3 The use of photographs as wallpaper is authorized, however, as with any other office display, employees should use good judgment and taste in placing these items on their computers.

5.7.4 Many kinds of software are available through the Internet. Virus free, shareware, freeware or other software may be used when approved by the IT Section. Copyright laws shall be observed at all times.

5.8 Records retention of electronic information is outlined in the ADVS E-mail Usage IMP 00-01.

5.8.1 The records retention requirements shall apply to all records obtained or received via the Internet.

5.8.2 ADVS employees who transmit or receive material via the Internet shall determine whether to preserve or delete the material and communication's consistent with the records retention schedule and records retention policy of ADVS.

5.9 ADVS employees with questions regarding records retention should contact the IT Section and/or review ARS §§ 41-1347, 41-1350, and 39-121.01(B).

5.9.1 Routine E-mail and communications (similar to oral conversation and voice mail, defined as expeditious communication on routine matters such as scheduling meetings and conference calls) may be deleted after the required action is taken.

5.10 Regulation and policy enforcement is ultimately the responsibility of the ADVS director.

5.10.1 The IT Section manager shall be responsible for agency compliance with the provisions of this policy and for investigating suspected incidents of non-compliance.

5.10.1.1 IT Section personnel are authorized to view material deemed unauthorized in section 5.3 of this policy for the purposes of monitoring and verification.

5.10.2 If in doubt, Internet users should seek policy clarification from an appropriate ADVS supervisory authority. Agency employees with questions regarding records retention should contact their

supervisor and refer to A.R.S. §§ 41-1347, 41-1350, and 39-121.01(B).

6.0 IMPLEMENTATION: This policy shall be implemented without change on the effective date.

_____

Ted Vogt, Director

ARIZONA DEPARTMENT OF VETERANS' SERVICES

INTERNAL MANAGEMENT POLICY 00-01

SUBJECT: E-MAIL USAGE

EFFECTIVE DATE: April 8, 2010 (Supersedes September 18, 2003)

1.0 POLICY: It is the policy of the Arizona Department of Veterans' Services (ADVS) to provide guidance on the proper use, preservation, disclosure and disposition of electronic mail. This policy, based on state law, describes the legitimate use of electronic mail with special emphasis on records-related issues.

2.0 AUTHORITY: A.R.S. § 41-604, Duties and powers of the (ADVS) director; § 41-3504.A.1.(13), Powers and duties of the (GITA) agency; violation; classification; and § 41-1350, Records definition.

3.0 RESPONSIBILITY: E-mail users are responsible for complying with this policy and attending annual E-mail training. The Information Technology (IT) Section is responsible for providing education on E-mail use and giving employees acknowledgment forms to be signed. Supervisors are responsible for notifying the IT Section when employees require initial training and collecting signed acknowledgments from employees. ADVS' Human Resources Section is responsible for filing acknowledgments in employees' personnel files. Violation of this policy may result in revocation of E-mail privileges and/or disciplinary action.

4.0 DEFINITIONS:

4.1 "E-Mail" means a communications tool (Electronic-mail) made available to certain agency employees for the performance of their duties. The purpose of E-mail is to provide expeditious communication among ADVS employees similar to oral conversation and voice mail.

4.2 "E-mail User" means an agency employee, contract employee or other agency-authorized person who accesses E-mail through the use of state/agency owned/controlled computer equipment.

4.3 "GITA" means Government IT Agency, the agency responsible for providing state agencies statewide guidelines on IT.

4.4 "Information Technology (IT)" means all computerized and auxiliary automated information processing, telecommunications and related technology, including hardware, software, vendor support and related services, equipment and projects.

4.5 "IT Section" means the ADVS office responsible for all aspects of IT for the agency (including E-mail accounts for agency personnel).

4.6 "Human Resources Section" means the ADVS office responsible for all aspects of Human Resource issues for the agency.

5.0 PROCEDURES: The IT Section manager shall be responsible for agency compliance with the provisions of this policy and for investigating suspected incidents of non-compliance. If in doubt, E-mail users should seek policy clarification from their direct supervisor or the IT Section.

5.0 E-mail users are responsible for complying with the following usage requirements in receiving/sending/maintaining E-mail messages:

5.0.1 Personnel should not use the ADVS internal E-mail system for personal use. If a user wishes to send personal correspondence, Internet based E-mail systems such as Hotmail, Yahoo and the like should be utilized instead.

5.0.2 All state employees with access to E-mail must acknowledge and consent that all network activity is the property of ADVS and the State of Arizona, and therefore, should not consider any E-mail activity to be private.

5.0.3 E-mail communications shall be professional in content; appropriate to a government agency; in compliance with agency and statewide policy; and consistent with other agency policies and procedures.

5.0.4 Agency work rules governing use of State property, record keeping and communications with others also apply to the use of E-mail. Users should never send an E-mail communication they would not feel comfortable communicating face-to-face or over the phone.

5.0.5 No E-mail communications shall be created or sent that might constitute discriminatory, harassing, intimidating, hostile or offensive communications based on gender, race, color, national origin, sexual orientation, disability, or other grounds.

5.0.6 Employees shall not read the E-mail of another employee without a legitimate business purpose consistent with the agency's policies and business communications practice.

5.0.7 No employee shall send E-mail under another person's name without that person's authorization, and the sender shall indicate his or her identity in the message.

5.0.8 Employees shall follow all security policies of the agency as set forth in section 5.3 of this internal management policy.

5.0.9 Generally, employees shall be expected to use reasonable judgment in the performance of their duties. Failure to do so may subject them to disciplinary procedures consistent with the policies of the agency.

5.1 E-mail for personal use:

5.1.1 Personnel should not use the ADVS internal E-mail system for personal use. If a user wishes to send personal correspondence, Internet based E-mail systems such as Hotmail, Yahoo and the like should be utilized instead.

5.1.2 Internet E-mail is subject to the same restrictions and guidelines as the ADVS Internet Usage IMP 00-02.

5.1.3 Users should not consider Internet based E-mail to be either private or secure.

5.1.4 Internet E-mail users should be aware ADVS monitors Internet use, including sites visited, without user consent and without prior notice.

5.1.5 Employees wishing to check personal E-mail accounts (e.g., Hotmail, Yahoo, or web mail from their ISP [Internet Service Provider]) using ADVS equipment should think about the content of any E-mail in their personal accounts prior to accessing it. If any content includes rude or offensive language, nudity or depictions of nudity, or sexual content, it should not be accessed.

5.2 E-mail is not secure. E-mail transmitted inside the agency is more secure than E-mail transmitted to state agencies on the Multiple Agency Network (MAGNET), and far more secure than E-mail transmitted via the Internet.

5.2.1 The agency may establish additional levels of security, ranging from password protection to authentication and encryption. The IT Section will work with supervisors to determine appropriate security levels for various E-mail accounts.

5.2.2 No Privacy in E-mail. Employees using E-mail shall have no expectation of privacy related to the use of this technology.

5.3 Ownership of E-mail. The E-mail accounts and the contents thereof are property of ADVS and the State of Arizona.

5.3.1 All messages created in the system belong to the State, not employees, vendors or customers.

5.3.2 The agency reserves the right to monitor E-mail use by any user at any time.

5.4 The E-mail user is responsible for determining which E-mail messages are records and which have no continuing value to the agency.

5.4.1 When an E-mail message is a record, then the E-mail message and related transmission and receipt data shall be retained in accordance with State statutes and approved records disposition schedules for the applicable record series. See section 5.7 below for additional information.

5.4.2 E-mail messages of only transitory value need not be saved. See section 5.7 below for additional information.

5.4.3 Agency management is responsible for creating and distributing E-mail records policies, appropriate to the agency's business needs and for implementing those policies, including training.

5.4.4 End users are responsible for managing E-mail messages they receive and properly identifying, classifying, retaining, and disposing of messages, in accordance with statewide and agency policies, as well as the technical means at their disposal.

5.5 Unacceptable use of agency E-mail. E-mail shall not be used for the following purposes:

5.5.1 Personal business or personal gain without authorization.
5.5.2 Soliciting.
5.5.3 Political campaigning.
5.5.4 Unethical, illegal, unprofessional or disruptive activities.
5.5.5 Any activity that would jeopardize the legitimate interests of the State or the citizens and Veterans' of the State of Arizona.

5.6 E-mail records retention and disposition. E-mail may be used to facilitate routine matters such as scheduling meetings and conference calls; notification of legal and policy issues to be resolved in more formal communication; requests for information; or directives to complete tasks; and notification of employees' whereabouts (e.g., vacations, conference, and out-of-office).

5.6.1 Employees who transmit E-mail shall determine whether to preserve or delete the E-mail communication, as follows:

5.6.1.1 Routine E-mail, of transitory value, may be deleted after the appropriate action is taken. No paper or computer record need be preserved unless the communication is subject to retention under this policy.

5.6.1.2 Communication that meets the definition of a record under A.R.S § 41-1350, transmitted inside the agency, or received from outside the agency, through the E-mail system, shall be printed and preserved in the appropriate file, in permanent paper format **or** preserved, unedited, in the E-mail system without printing.

5.6.1.2.1 An excerpt from the statute that defines "record" reads, "made or received by any governmental agency in pursuance of law or in connection with the transaction of public business and preserved or appropriate for preservation by the agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the government, or because of the informational and historical value of data contained therein."

5.6.1.2.2 With every communication that qualifies as a record, the sender shall, ensure that:

5.6.1.2.2.1 The time and date the message was sent and received; the complete sender and receiver identification, and; the complete message, are preserved.

5.6.1.2.2.2 The E-mail may be preserved as any other type of record by being either

printed out and preserved in the hardcopy file, **or** preserved in an electronic archive.

5.6.2 Communications subject to an existing public records request, or to formal discovery in ongoing litigation, will be preserved in the appropriate file or the E-mail system.

5.7 IT Section responsibilities relative to E-mail:

5.7.1 E-mail systems will be backed up regularly.

5.7.1.1 The E-mail data backup will be deleted pursuant to the Department of Library, Archives and Public Records' approved Records Disposition Schedule for the agency.

5.7.1.2 The IT Section will document its schedule for E-mail backup and provide a copy of the systems backup to GITA.

5.7.1.3 Periodic record of E-mail system address books and distribution lists will be retained pursuant to the Department of Library, Archives and Public Records' approved Records Disposition Schedule for the agency.

5.7.2 Employees will be provided with E-mail use policies.

5.7.2.1 New employees shall not be granted access to the E-mail system until they have received training.

5.7.2.2 E-mail training shall, at least once per year, be provided to all employees interested in attending.

5.7.3 ADVS shall, at least once per year, perform a random documented audit of employee E-mail use.

5.7.3.1 The audit shall, at a minimum, include review of E-mail messages transmitted and received by a reasonable percentage of E-mail users, to be determined by the ADVS director.

5.7.3.2 The IT manager may access E-mail, at any time, to ensure compliance with this policy.

5.7.3.3 Agency employees with questions regarding records retention should contact their supervisor and refer to A.R.S. §§ 41-1347, 41-1350, and 39-121.01(B).

5.7.3.4 If in doubt, Internet users should seek policy clarification from an appropriate ADVS supervisory authority.

6.0 IMPLEMENTATION: This policy shall be implemented without change on the effective date.

_____

Ted Vogt, Director

ARIZONA DEPARTMENT OF VETERANS' SERVICES
INTERNAL MANAGEMENT POLICY 13-01

SUBJECT: **MOBILE DEVICE USAGE AND SECURITY**

EFFECTIVE DATE: August 5, 2013

This policy does not create a contract for employment between any ADVS employee and the Department. Nothing in this policy changes the fact that all uncovered employees of the Department are at-will employees and serve at the pleasure of the appointing authority.

POLICY

It is the policy of the Arizona Department of Veterans' Services (ADVS) to provide employees with mobile device access and guidance on its use. Mobile devices are a communications tool made available to selected ADVS employees to enhance performance of their duties. Its use should be managed by rules of conduct applicable to any other Information Technology (IT) resource.

AUTHORITY

§41-3504.A.1 (13), Powers and duties of the (GITA) agency; violation; classification
R2-5A-501, Standards of Conduct

RESPONSIBILITY

Mobile device users shall comply with all applicable federal and state laws, including A.R.S. §38-448 and ADVS policies, procedures and guidelines. The IT Section is responsible for providing education on mobile device usage and giving employees acknowledgement forms to be signed. Supervisors are responsible for notifying the IT Section when employees require mobile devices and collecting signed acknowledgement forms from employees. The ADVS Human Resources Section is responsible for filing acknowledgements in the official personnel file. Violation of this policy may result in revocation of the privilege to access the Internet and/or disciplinary action.

DEFINITIONS

"Information Technology (IT)" means all computerized and auxiliary automated information processing, telecommunications and related technology, including hardware, software, vendor support and related services, equipment and projects.

"IT Section" means the ADVS office responsible for all aspects of IT for the agency (including Internet access for the agency).

"Human Resources Section" means the ADVS office responsible for all aspects of Human Resource issues for the agency.

"Mobile Device" refers to laptop/notebook/tablet computers, Ultra-mobile PCs (UMPC), mobile/cellular phones, Smartphones, PDAs, home or personal computers used to access corporate resources and any mobile device capable of storing corporate data and connecting to an unmanaged network.

"Internet User" means an agency employee, contract employee or other agency-authorized person who accesses the Internet through the use of state/agency owned/controlled computer equipment.

PURPOSE

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data from a mobile device connected to an unmanaged network outside of ADVS' direct control.

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 client and business data that resides within ADVS' technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be accessed by unsanctioned sources. A breach of this type could result in loss of personal identifiable information (PII), damage to critical applications, loss of revenue, and damage to the company's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of ADVS' direct control to backup, store, and otherwise access corporate data of any type must adhere to company-defined processes for doing so.

APPLICABILITY

This policy applies to all ADVS employees, including full and part-time staff, contractors, freelancers, and other agents who utilize either company-owned or personally-owned mobile devices to access, store, back up or relocate any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust ADVS has built with its clients, supply chain partners and other constituents. Consequently, employment at ADVS does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

It addresses a range of threats to – or related to the use of – enterprise data:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive corporate data could be deliberately stolen and sold by an employee.
Copyright	Software copied onto a mobile device could violate licensing.
Malware	Viruses, Trojans, Worms, Spyware and other threats could be introduced via a mobile device.
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 mobile device connectivity will be managed at the sole discretion of IT. Non-sanctioned use of mobile devices to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the enterprise network.

RESPONSIBILITIES

The Director of ADVS has the overall responsibility for the confidentiality, integrity, and availability of corporate data. The Director has delegated the execution and maintenance of Information Technology and Information Systems to the Chief Information Officer. Other IT staff members under the direction of the CIO are responsible for following the procedures and policies within Information Technology and Information Systems. All ADVS employees are responsible to act in accordance with company policies and procedures.

POLICY AND APPROPRIATE USE

It is the responsibility of any employee of ADVS who uses a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct ADVS business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

ACCESS CONTROL

IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the company's systems, data, users, or clients at risk or violates any ADVS policies and procedures.

Prior to initial use on the corporate network or related infrastructure, all mobile devices must be registered with IT.

End users who wish to connect such devices to non-corporate network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, antivirus software and any other security measure deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet ADVS established enterprise IT security standards.

End users who wish to use personal equipment, cell phones or tablets, to access agency Email also must agree that IT has their permission to issue a "remote wipe" of the device if the device is lost or stolen. This will not only remove the agency Email account from the device, but will also remove any pictures, music or any other data stored locally in the device.

All mobile devices attempting to connect to the corporate network through an unmanaged network (i.e. the Internet) will be inspected by the ADVS IT department. Devices that have not been previously approved by IT, are not in compliance with IT's security policies, or represent any threat to the corporate network or data will not be allowed to connect. Laptop computers or personal PCs may not access the corporate network and data.

SECURITY

Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password. Employees agree to never disclose their passwords to anyone, particularly to family members, if business work is conducted from home.

All users of mobile devices 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 and physical control of such devices whenever they contain enterprise data. Any non-corporate computers used to

synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by the ADVS IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.

Passwords and other confidential data as defined by the ADVS IT department are not to be stored unencrypted on mobile devices.

Any mobile device that is being used to store ADVS data must be in compliance with the authentication requirements of the ADVS IT department. In addition, all hardware security configurations (personal or company-owned) must be pre-approved by the ADVS IT department before any enterprise data-carrying device can be connected to it.

IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with the ADVS overarching security policy.

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.

In the event of a lost or stolen mobile device, it is incumbent on the user to report this to the IT department immediately.

Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace. This applies to both corporate-owned and personal mobile devices being used within the company premises.

HELP AND SUPPORT

The ADVS IT department will support its sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT department.

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 the ADVS IT department. This includes, but is not limited to, any reconfiguration of the mobile device.

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 enterprise network.

ORGANIZATIONAL AND REPORTING PROTOCOL

The end user agrees to immediately report to his/her manager or supervisor and the ADVS IT department any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.

ADVS will not reimburse employees if they choose to purchase their own mobile devices.

Every mobile device user will be entitled to a training session around this policy. While a mobile device user will not be granted access to corporate resources using a mobile device without accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

POLICY NON-COMPLIANCE

Failure to comply with the Mobile Device Usage and Security Policy may, at the full discretion of ADVS, result in the suspension of any or all technology use and connectivity privileges.

The State Personnel System rules pertaining to Standards of Conduct (R2-5A-501) require state employees to comply with agency policies and directives. Noncompliance with the Standards of Conduct may result in discipline or separation from employment. In addition, any non-compliance with this Standard that may constitute a violation of State or Federal criminal statute may be referred to a law enforcement agency for appropriate action.

Contractors and other authorized users will be held to contractual agreements. In addition, any non-compliance with this policy that may constitute a violation of a State or Federal criminal statute may be referred to a law enforcement agency for appropriate action.

IMPLEMENTATION

This policy shall be implemented without change on the effective date.

Ted Vogt, Director

ADVS Acknowledgment for Transfer of Accountability

In accordance with Statewide Standard P800-S885 Rev.1.0 Section 4.4 & Statewide Standard P800-815 Section 4.1.2, the Arizona Department of Veterans' Services (ADVS) Information Technology department (I.T. Department) will use this form as acknowledgment for transfer of accountability for portable end-user hardware and software as defined by Statewide Standard P800-815 Section 4.2.2.

By verifying the information and signing below, you are acknowledging that you assume all risks and responsibility of equipment issued by the I.T. Department. In order to prevent theft/loss of such equipment and potentially confidential information, the equipment holder shall abide by the following procedures:

1) Equipment will only be issued to supervisory/leadership. From there, it is up to their discretion who is able to have use of it.
2) It will be equipment holder's responsibility to ensure that the device(s) are securely stored when not in use by staff.
3) Any loss of device due to theft/damages will be IMMEDIATELY reported to I.T. staff. Those found guilty of theft will be held liable pursuant to ADVS policies and ARS Title 13 Chapter 18.
4) The I.T. department reserves the right to revoke use of devices if intentional misuse or violation I.T. polices (specifically the mobile device policy) and procedures is suspected.

Additionally, if for any reason the below signee is no longer attached to ADVS, equipment must be returned to I.T. department by that person or persons' direct supervisor and/or acting authority.

This form is intended for use for ADVS portable end-user hardware and software only. All other devices are not covered by any terms and conditions of this document.

Issuer	**Recipient**
_____	_____
Signature	Signature
_____	_____
Date	Date

Device Model	Serial Number	AZ Tag

Title 38, ARS §38-448

Be it enacted by the Legislature of the State of Arizona:

Section 1. Title 38, chapter 3, article 4, Arizona Revised Statutes, is amended by adding section 38-448, to read:

38-448. State employees; access to internet pornography prohibited; cause for dismissal; definitions

A. EXCEPT TO THE EXTENT REQUIRED IN CONJUNCTION WITH A BONA FIDE, AGENCY APPROVED RESEARCH PROJECT OR OTHER AGENCY APPROVED UNDERTAKING, AN EMPLOYEE OF AN AGENCY SHALL NOT KNOWINGLY USE AGENCY OWNED OR AGENCY LEASED COMPUTER EQUIPMENT TO ACCESS, DOWNLOAD, PRINT OR STORE ANY INFORMATION INFRASTRUCTURE FILES OR SERVICES THAT DEPICT NUDITY, SEXUAL ACTIVITY, SEXUAL EXCITEMENT OR ULTIMATE SEXUAL ACTS AS DEFINED IN SECTION 13-3501. AGENCY HEADS SHALL GIVE, IN WRITING, ANY AGENCY APPROVALS. AGENCY APPROVALS ARE AVAILABLE FOR PUBLIC INSPECTION PURSUANT TO SECTION 39-121.

B. AN EMPLOYEE WHO VIOLATES THIS SECTION PERFORMS AN ACT THAT IS CAUSE FOR DISCIPLINE OR DISMISSAL OF THE EMPLOYEE AND FOR AN EMPLOYEE IN STATE SERVICE IS CONSIDERED MISUSE OR UNAUTHORIZED USE OF STATE PROPERTY PURSUANT TO SECTION 41-770.

C. ALL AGENCIES SHALL IMMEDIATELY FURNISH THEIR CURRENT EMPLOYEES WITH COPIES OF THIS SECTION. ALL AGENCIES SHALL FURNISH ALL NEW EMPLOYEES WITH COPIES OF THIS SECTION AT THE TIME OF AUTHORIZING AN EMPLOYEE TO USE AN AGENCY COMPUTER.

D. FOR THE PURPOSES OF THIS SECTION:

1. "AGENCY" MEANS:

(a) ALL OFFICES, AGENCIES, DEPARTMENTS, BOARDS, COUNCILS OR COMMISSIONS OF THIS STATE.

(b) ALL STATE UNIVERSITIES.

(c) ALL COMMUNITY COLLEGE DISTRICTS.

(d) ALL LEGISLATIVE AGENCIES.

(e) ALL DEPARTMENTS OR AGENCIES OF THE STATE SUPREME COURT OR THE COURT OF APPEALS.

2. "INFORMATION INFRASTRUCTURE" MEANS TELECOMMUNICATIONS, CABLE AND COMPUTER NETWORKS AND INCLUDES THE INTERNET, THE WORLDWIDE WEB, USENET, BULLETIN BOARD SYSTEMS, ON-LINE SYSTEMS AND TELEPHONE NETWORKS.

APPROVED BY THE GOVERNOR APRIL 17, 2003.

FILED IN THE OFFICE OF THE SECRETARY OF STATE APRIL 18, 2003.

ARIZONA DEPARTMENT OF VETERANS' SERVICES

USE AFFIRMATION STATEMENT

EFFECTIVE DATE: April 8, 2010 (Supersedes October 1st, 2003)

I have been made aware and understand that all personnel who have access to ADVS data, computers, E-mail and network resources are bound by applicable laws, rules and ADVS policies regarding. I agree to abide by all applicable laws, rules and ADVS policies, and I pledge to refrain from any and all of the following:

1. Revealing ADVS data to any person or persons outside or within ADVS who have not been specifically authorized to receive such data.
2. Storing any Personal Identifiable Information, agency sensitive data or data that would violate any HIPPA Privacy Laws on portable media is strictly prohibited. Portable media includes but is not limited to: flash drives, "thumb" drives, external USB hard drives, and CDRW or DVDRW media.
3. Attempting or achieving access to ADVS data not germane to my mandated job functions.
4. Entering/altering/erasing ADVS data maliciously or in retribution for real or imagined abuse, or for personal amusement.
5. Entering/altering/erasing ADVS data for direct or indirect personal gain or advantage.
6. Using ADVS terminals, printers, and/or other equipment inappropriately.
7. Using another person's personal ADVS logon ID and password.
8. Revealing my personal ADVS logon ID and password to any unauthorized personnel.
9. Asking another user to reveal his/her personal ADVS login ID and password.

In relation to my responsibilities regarding proprietary rights of the authors or computer software utilized by ADVS, I recognize that:

1. ADVS licenses the use of computer software from a variety of outside companies. ADVS does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce or alter the software or the documentation.
2. When used on a local area network or on multiple machines, ADVS employees shall use the software in accordance with the license agreement.
3. ADVS employees who know of any misuse of software or related documentation within the agency shall notify their manager/supervisor or the IT Section.
4. ADVS employees making, acquiring or using unauthorized copies of computer software are subject to disciplinary action in accordance with Internal Management Policy 00-02.
5. According to U.S. Copyright Law, 17 USC Sections 101 and 506, illegal reproduction of software can be subject to criminal damages up to $250,000 and/or up to 5 years imprisonment.
6. In the event that an employee is sued or prosecuted for the illegal reproduction of software, he/she will not be represented by ADVS or the Arizona Attorney General.

Appropriate action will be taken to ensure that applicable federal and state laws, regulations, and ADVS policies governing confidentiality and security are enforced. A breach of procedure occurring pursuant to this policy or misuse of department property

including computer programs, equipment and/or data may result in disciplinary action, including dismissal, and/or prosecution in accordance with any applicable provision of law.

My signature below confirms that I have read and accept responsibility for adhering to all applicable laws, rules, regulations and ADVS policies. Failure to sign this statement will mean that I will be denied access to ADVS data, computer equipment and software.

Signature: _____ Date: _____

PLEASE SIGN AND RETURN TO:
Arizona Department of Veterans' Services
IT SECTION

ARIZONA DEPARTMENT OF VETERANS' SERVICES

INTERNET USAGE POLICY ACKNOWLEDGEMENT FORM

EFFECTIVE DATE: April 8, 2010 (Supersedes October 1st, 2003)

I, _____, have read and understand the Internet Usage Internal Management Policy 00-02 for the Arizona Department of Veterans' Services and been provided with a copy of A.R.S. § 38-448. I agree to comply with all terms and conditions of this policy and statute.

I also understand and agree that all Internet, network and information systems activity conducted with state/agency resources is the property of the Arizona Department of Veterans' Services and the State of Arizona.

I understand that the Arizona Department of Veterans' Services reserves the right to monitor and log all network activity, including Internet access, with or without notice. I have no expectation of privacy in the use of these resources.

Signed: _____

Date: _____

I agree that the above mentioned employee requires Internet access to complete their job function more efficiently.

Division Head: _____

Signed: _____

Date: _____

LIABILITY
The Arizona Department of Veterans' Services makes no warranties of any kind, whether express or implied, for the use of the Internet or electronic information resources. Additionally, the Arizona Department of Veterans' Services is not responsible for any damages whatsoever that employees may suffer arising from or related to use of the Internet or electronic information resources.

PLEASE SIGN AND RETURN TO:
Arizona Department of Veterans' Services
IT SECTION

ARIZONA DEPARTMENT OF VETERANS' SERVICES

E-MAIL USAGE POLICY ACKNOWLEDGEMENT FORM

EFFECTIVE DATE: April (Supersedes October 1st, 2003)

I, _____, have read and understand the E-mail Usage Internal Management Policy 00-01 for the Arizona Department of Veterans' Services. I agree to comply with all terms and conditions of this policy.

I understand and agree that all Internet, network and information systems activity conducted with state/agency resources is the property of the Arizona Department of Veterans' Services and the State of Arizona.

I understand that the Arizona Department of Veterans' Services reserves the right to monitor and log all network activity, including E-mail, with or without prior consent or notice. I have no expectation of privacy in the use of these resources.

Signed:

_____Date:_____

LIABILITY

The Arizona Department of Veterans' Services makes no warranties of any kind, whether express or implied, for the use of the E-mail system or electronic information resources. Additionally, the Arizona Department of Veterans' Services is not responsible for any damages whatsoever that employees may suffer arising from or related to use of E-mail or electronic information resources.

PLEASE SIGN AND RETURN TO:
Arizona Department of Veterans' Services
IT SECTION

ARIZONA DEPARTMENT OF VETERANS' SERVICES

MOBILE DEVICE USAGE POLICY ACKNOWLEDGEMENT FORM

EFFECTIVE DATE: April 8, 2010 (Supersedes October 1st, 2003)

I, _____, have read and understand the Mobile Device Usage Internal Management Policy 00-04 for the Arizona Department of Veterans' Services. I agree to comply with all terms and conditions of this policy. Violation of this policy may resulting revocation of the privilege and/or disciplinary action.
.

I understand mobile device usage is a service and is the property of ADVS and the State of Arizona. ADVS reserves the right to monitor Cell phone use by any user at any time. The ADVS Director or Purchasing Office manager may determine appropriate use and deny, revoke, suspend or close any user account at any time, based upon a determination of inappropriate use.

Signed:

_____Date:_____

LIABILITY

Employees who are charged with traffic violations resulting from the use of their phone while driving will be solely responsible for all liabilities that result from such actions.

PLEASE SIGN AND RETURN TO:
Arizona Department of Veterans' Services
IT SECTION