INFORMATION SECURITY POLICY

This Policy applies to ARG EUROPE LTD // ARG SURVEYS LTD // ARG CONTRACTS LTD

V.Blair
1st February 2024

ARG Group
Unit 2 New Ford Road
Waltham Cross
EN8 7PG

Tel: 0208 804 8008
Email: enquiries@arggroup.org

TABLE OF CONTENTS

1 Introduction

This Policy refers to the ARG GROUP. The ARG GROUP is the name given to the collective companies ARG EUROPE LTD, ARG CONTRACTS LTD, FIBRE CLEAR CONSULTING LTD. This Policy applies to all under the ARG GROUP Banner

1.1 Purpose

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at ARG Group. It serves as a central policy document with which all employees and contractors must be familiar and defines actions and prohibitions that all users must follow. The policy provides employees with policies and guidelines concerning the acceptable use of ARG technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all employees or temporary workers at all locations and by contractors working for the company as subcontractors.

1.2 Scope

This policy document defines common security requirements for all personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of ARG Group, entities in the private sector, in cases where the company has a legal, contractual or fiduciary duty to protect said resources while in the company custody. In the event of a conflict, the more restrictive measures apply. This policy covers the company's network system which is comprised of various hardware, software, communication equipment and other devices designed to assist the business in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any ARG domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by the business at its office locations or at remote locales.

1.3 Acronyms / Definitions

Common terms and acronyms that may be used throughout this document.

MD – The Managing Director is responsible for the overall privacy and security ARGs of the company.
CM – The Compliance Manager is responsible for annual security training of all staff on confidentiality issues and any privacy compliance issues.
Encryption – The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific 'need to know.'
External Media –i.e. CD-ROMs, DVDs, floppy disks, flash drives, USB keys, and thumb drives, tapes
FAT – File Allocation Table - The FAT file system is relatively uncomplicated and an ideal format for floppy disks and solid-state memory cards. The most common implementations have a serious drawback in that when files are deleted and new files written to the media, their fragments tend to become scattered over the entire media, making reading and writing a slow process.
Firewall – a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.
FTP – File Transfer Protocol
IT - Information Technology

LAN – Local Area Network – a computer network that covers a small geographic area, i.e. a group of buildings, an office.
NTFS – New Technology File Systems **–** NTFS has improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization plus additional extensions such as security access control lists and file system journaling. The exact specification is a trade secret of Microsoft.
SOW - Statement of Work - An agreement between two or more parties that details the working relationship between the parties and lists a body of work to be completed.
User - Any person authorized to access an information resource.
Privileged Users – system administrators and others specifically identified and authorized by ARG management.
Users with edit/update capabilities – individuals who are permitted, based on job assignment, to add, delete, or change records in a database**.**
Users with inquiry (read only) capabilities – individuals who are prevented, based on job assignment, from adding, deleting, or changing records in a database. Their system access is limited to reading information only.
VLAN – Virtual Local Area Network – A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.
VPN – Virtual Private Network – Provides a secure passage through the public Internet.
WAN – Wide Area Network – A computer network that enables communication across a broad area, i.e. regional, national.
Virus – a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

1.4 Compliance Manager

The Compliance Manager or their appointed deputy will oversee all ongoing activities related to the development, implementation, and maintenance of the company policies in accordance with applicable laws. The Compliance Manager is:

Victoria Blair
Vickyblair@arggroup.org

The MD and CM will meet quarterly or as required to discuss security issues and to review concerns that arose during the quarter. They will identify areas that should be addressed during annual training and review/update security policies as necessary.

The MD will address security issues as they arise and recommend and approve immediate security actions to be undertaken. It is the responsibility of the CM to identify areas of concern within the company and act as the first line of defense in enhancing the security posture of the business.

The CM is responsible for maintaining a log of security concerns or confidentiality issues. This log must be maintained on a routine basis, and must include the dates of an event, the actions taken to address the event, and recommendations for personnel actions, if appropriate. This log will be reviewed during the annual Management review meeting.

2 Employee Responsibilities

2.1 Employee Requirements

The first line of defense in data security is the individual user. Users are responsible for the security of all data which may come to them in whatever format. The CM is responsible for maintaining ongoing training programs to inform all users of these requirements.

Wear Identifying Badge so that it may be easily viewed by others **–** When working on site, In order to help maintain security, all employees should prominently display their employee identification badge.

Challenge Unrecognized Personnel **-** It is the responsibility of all employees to take positive action to provide physical security. If you see an unrecognized person in a restricted location, you should challenge them as to their right to be there. All visitors to company sites must sign. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

Secure iPad / Tablets **-** When out of the office / on site all iPads / Tablets must be secured when not in use. iPads / Tablets are unfortunately easy to steal and may contain sensitive company information.

Unattended Computers **-** Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during security training. Company policy states that all computers will have the automatic screen lock function set to automatically activate upon Ten minutes of inactivity. Employees are not allowed to take any action which would override this setting.

Home Use of Company Corporate Assets - Only computer hardware and software owned by and installed by ARG is permitted to be connected to or installed on company equipment. Only software that has been approved for corporate use by the company may be installed on company equipment. Personal computers / iPads / Tablets supplied by the company are to be used solely for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by the company for home use.

Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of ARG are the property of the company unless covered by a contractual agreement. Nothing contained herein applies to software purchased by ARG employees at their own expense.

2.2 Prohibited Activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.
- Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.
- Exception: Authorized information system support personnel, or others authorized by ARG Privacy Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.

- Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
- Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on ARG computers must be approved by ARG. This also applies to downloading of applications to tablet / phones without prior authorisation.
- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by ARG is strictly prohibited.
- System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of ARG is strictly prohibited.

2.3 Electronic Communication, E-mail, Internet Usage

As a productivity enhancement tool, the company encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by ARG owned equipment are considered the property of ARG – not the property of individual users. Consequently, this policy applies to all ARG employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, and servers.

ARG provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. However, incidental personal use is permissible as long as:

1) it does not consume more than a trivial amount of employee time or resources,
2) it does not interfere with staff productivity,
3) it does not preempt any business activity,
4) it does not violate any of the following:

a) Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
b) Illegal activities – Use of ARG information resources for or in support of illegal purposes as defined by regulation or law is strictly prohibited.
c) Commercial use – Use of ARG information resources for personal or commercial profit is strictly prohibited.
d) Political Activities – All political activities are strictly prohibited on ARG premises. ARG encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using ARG assets or resources.
e) Harassment – ARG strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, ARG prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.
f) Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when

someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

Generally, while it is **NOT** the policy of ARG to monitor the content of any electronic communication, ARG is responsible for servicing and protecting ARG's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

ARG reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as ARG policies.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

2.4 Internet Access

Internet access is provided for ARG users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by ARG should not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, etc. Do not use the Internet as a radio or to constantly monitor the weather or stock market results. While seemingly trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by ARG routers and firewalls. This list is constantly monitored and updated as necessary. Any employee visiting pornographic sites will be disciplined and may be terminated.

2.5 Reporting Software Malfunctions

Users should inform the appropriate ARG personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, ARG computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer.
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.

- Inform the appropriate personnel or ARG ISO as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

The ISO should monitor the resolution of the malfunction or incident, and report to the CST the result of the action with recommendations on action steps to avert future similar occurrences.

2.6 Report Security Incidents

It is the responsibility of each ARG employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or security person. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately to the Privacy Officer Users should report any perceived security incident to either their immediate supervisor, or to their department head.

Reports of security incidents shall be escalated as quickly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged, and the remedial action indicated.

Security breaches shall be promptly investigated. If criminal action is suspected, ARG Privacy Officer shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

2.7 Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by ARG and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of ARG policy and will result in personnel action and may result in legal action.

2.8 Transferring Software and Files between Home and Work

Personal software shall not be used on ARG computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use ARG purchased software on home or on non-ARG computers or equipment.

ARG proprietary data, including but not limited to IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of ARG without written consent of the respective supervisor or department head. It is crucial to ARG to protect all data and, in order to do that effectively we must control the systems in which it is contained. In the event that a supervisor or department head receives a request to transfer ARG data to a non-ARG Computer System, the supervisor or department head should notify the appropriate personnel of the intentions and the need for such a transfer of data.

ARG Wide Area Network ("WAN") is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Since ARG does not control non-ARG personal computers, ARG cannot be sure of the

methods that may or may not be in place to protect ARG sensitive information, hence the need for this restriction.

2.9 Internet Considerations

Special precautions are required to block Internet (public) access to ARG information resources not intended for public access, and to protect confidential ARG information when it is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage.

Prior approval of ARG Privacy Officer or appropriate personnel authorized by ARG shall be obtained before:

- An Internet, or other external network connection, is established;
- ARG information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g. web or ftp server) or device;
- Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact their supervisor;
- Use shall be consistent with the goals of ARG. The network can be used to market services related to ARG, however use of the network for personal profit or gain is prohibited.
- Confidential or sensitive data - including credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.
- The encryption software used, and the specific encryption keys (e.g. passwords, pass phrases), shall be escrowed with ARG Privacy Officer or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

2.10 Installation of authentication and encryption certificates on the e-mail system

Any user desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user. Once verified, the certificate is installed on both recipients' workstations, and the two may safely exchange secure e-mail.

2.11 Use of WinZip encrypted and zipped e-mail

This software allows ARG personnel to exchange e-mail with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any ARG staff member who desires to utilize this technology may request this software from the Privacy Officer or appropriate personnel.

3 Identification and Authentication

3.1 User Logon IDs

Individual users shall have unique logon IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use and misuse of their individual logon ID.

All user login IDs are audited at least twice yearly and all inactive logon IDs are revoked. ARG Human Resources Department notifies the CM or appropriate personnel upon the departure of all employees and contractors, at which time login IDs are revoked.

The logon ID is locked or revoked after a maximum of three unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

3.2 Passwords

User Account Passwords
User IDs and passwords are required in order to gain access to all ARG networks and workstations. All passwords are restricted by a corporate-wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password in order to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

Password Length – Passwords are set at the start of employment by the CM.

Content Requirements - Passwords must contain a combination of upper and lower case alphabetic characters.

Restrictions on Sharing Passwords - Passwords shall not be shared, written down on paper, or stored within a file or database on a workstation and must be kept confidential.

Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens, and are never printed or included in reports or logs. Passwords are stored in an encrypted format.

3.3 Confidentiality Agreement

Users of ARG information resources shall sign, as a condition for employment, an appropriate confidentiality agreement. The agreement shall include the following statement, or a paraphrase of it:

> *I understand that any unauthorized use or disclosure of information residing on ARG information resource systems may result in disciplinary action consistent with the policies and procedures of the company and applicable regulations.*

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing ARG information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or employees are leaving an organization.

3.4 Access Control

Information resources are protected by the use of access control systems. Access control systems include both internal (i.e. passwords, encryption, access control lists, constrained user interfaces, etc.) and external (i.e. port protection devices, firewalls, host-based authentication, etc.).

Rules for access to resources (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the resources.

Users may be added to the information system or network, upon the signature of the appropriate personnel who is responsible for adding the employee to the network in a manner and fashion that ensures the employee is granted access to data only as specifically requested.

Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited and that violators will be subject to criminal prosecution.

Identification and Authentication Requirements

The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session is subject to the authorization process previously addressed.

3.5 Termination of User Logon Account

Upon termination of an employee, whether voluntary or involuntary, employee's supervisor or department head shall notify the CM. The employee's department head shall be responsible for insuring that all keys, ID badges, and other access devices as well as ARG equipment and property is returned to ARG prior to the employee leaving ARG on their final day of employment.

4 Network Connectivity

4.1 Dial-In Connections

Access to ARG information resources through modems or other dial-in devices / software, if available, shall be subject to authorization and authentication by an access control system. **Direct inward dialing without passing through the access control system is prohibited.**

Systems that allow public access to host computers, including mission-critical servers, warrants additional security at the operating system and application levels. Such systems shall have the capability to monitor activity levels to ensure that public usage does not unacceptably degrade system responsiveness.

Dial-up access privileges are granted only upon the request of a department head with the submission of the Network Access Form and the approval of the Privacy Officer or appropriate personnel.

4.2 Dial Out Connections

ARG provides a link to an Internet Service Provider. If a user has a specific need to link with an outside computer or network through a direct link, approval must be obtained from the Privacy Officer or appropriate personnel. The appropriate personnel will ensure adequate security measures are in place.

4.3 Telecommunication Equipment

Certain direct link connections may require a dedicated or leased phone line. These facilities are authorized only by the Privacy Officer or appropriate personnel and ordered by the appropriate personnel. Telecommunication equipment and services include but are not limited to the following:

- phone lines
- fax lines
- calling cards
- phone head sets
- software type phones installed on workstations
- conference calling contracts
- cell phones
- Blackberry type devices
- call routing software
- call reporting software
- phone system administration equipment
- T1/Network lines
- long distance lines
- 800 lines
- local phone lines
- PRI circuits
- telephone equipment

4.4 Permanent Connections

The security of ARG systems can be jeopardized from third party locations if security ARGs and resources are inadequate. When there is a need to connect to a third party location, a risk analysis should be

conducted. The risk analysis should consider the type of access required, the value of the information, the security measures employed by the third party, and the implications for the security of ARG systems. The Privacy Officer or appropriate personnel should be involved in the process, design and approval.

4.5 Emphasis on Security in Third Party Contracts

Access to ARG computer systems or corporate networks should not be granted until a review of the following concerns have been made, and appropriate restrictions or covenants included in a statement of work ("SOW") with the party requesting access.

- Applicable sections of ARG Information Security Policy have been reviewed and considered.
- Policies and standards established in ARG information security program have been enforced.
- A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- The right to audit contractual responsibilities should be included in the agreement or SOW.
- A description of each service to be made available.
- Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.
- A detailed list of users that have access to ARG computer systems must be maintained and auditable.
- If required under the contract, permission should be sought to screen authorized users.
- Dates and times when the service is to be available should be agreed upon in advance.
- Procedures regarding protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
- The right to monitor and revoke user activity should be included in each agreement.
- Language on restrictions on copying and disclosing information should be included in all agreements.
- Responsibilities regarding hardware and software installation and maintenance should be understood and agreement upon in advance.
- Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
- If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
- A formal method to grant and authorized users who will access to the data collected under the agreement should be formally established before any users are granted access.
- Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.
- Because annual confidentiality training is required under regulation, a formal procedure should be established to ensure that the training takes place, that there is a method to determine who must take the training, who will administer the training, and the process to determine the content of the training established.
- A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.

4.6 Firewalls

Authority from the Privacy Officer or appropriate personnel must be received before any employee or contractor is granted access to a ARG router or firewall.

5 Malicious Code

5.1 Antivirus Software Installation

Antivirus software is installed on all ARG personal computers and servers. Virus update patterns are updated daily on ARG servers and workstations. Virus update engines and data files are monitored by appropriate administrative staff that is responsible for keeping all virus patterns up to date.

Configuration **-** The antivirus software currently implemented by ARG is Symantec. Updates are received directly from Symantec which is scheduled daily.

Remote Deployment Configuration **-** Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as needed basis.

Monitoring/Reporting – A record of virus patterns for all workstations and servers on ARG network may be maintained. Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the Privacy Officer or appropriate personnel.

5.2 New Software Distribution

Only software created by ARG application staff, if applicable, or software approved by the Privacy Officer or appropriate personnel will be used on internal computers and networks. A list of approved software is maintained. All new software will be tested by appropriate personnel in order to ensure compatibility with currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from electronic bulletin boards, the Internet, or on disks (magnetic or CD-ROM and custom-developed software).

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the Privacy Officer or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on ARG computers and networks. These precautions include determining that the software does not, because of faulty design, "misbehave" and interfere with or damage ARG hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a ARG computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate ARG personnel for instructions for scanning files for viruses.

Every diskette, CD-ROM, DVD and USB device is a potential source for a computer virus. Therefore, every diskette, CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a ARG computer or network.

Computers shall never be "booted" from a diskette, CD-ROM, DVD or USB device received from an outside source. Users shall always remove any diskette, CD-ROM, DVD or USB device from the computer when not in use. This is to ensure that the diskette, CD-ROM, DVD or USB device is not in the computer when the machine is powered on. A diskette, CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the diskette, CD_ROM, DVD or USB device is not "bootable".

5.3 Retention of Ownership

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of ARG are the property of ARG unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging ARG ownership at the time of employment. Nothing contained herein applies to software purchased by ARG employees at their own expense.

6 Encryption

6.1 Definition

Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To readhttp://www.webopedia.com/TERM/e/read.html an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

6.2 Encryption Key

An encryption key specifies the particular transformation of plain text into cipher text, or vice versa during decryption.

If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, ARG shall establish the criteria in conjunction with the Privacy Officer or appropriate personnel. ARG employs several methods of secure data transmission.

6.3 Installation of authentication and encryption certificates on the e-mail system

Any user desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user by contacting the Privacy Officer or appropriate personnel. Once verified, the certificate is installed on each recipient workstation, and the two may safely exchange secure e-mail.

6.4 Use of WinZip encrypted and zipped e-mail

This software allows ARG personnel to exchange e-mail with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any ARG staff member who desires to utilize this technology may request this software from the Privacy Officer or appropriate personnel.

6.5 File Transfer Protocol (FTP)

Files may be transferred to secure FTP sites through the use of appropriate security precautions. Requests for any FTP transfers should be directed to the Privacy Officer or appropriate personnel.

7 Building Security

It is the policy of ARG to provide building access in a secure manner. Each site, if applicable, is somewhat unique in terms of building ownership, lease contracts, entranceway access, fire escape requirements, and server room control. However, ARG strives to continuously upgrade and expand its security and to enhance protection of its assets and medical information that has been entrusted to it. The following list identifies measures that are in effect at ARG. All other facilities, if applicable, have similar security appropriate for that location.

- Entrance to the building during non-working hours is controlled by a security code system. Attempted entrance without this code results in immediate notification to the police department.
- Only specific ARG employees are given the security code for entrance. Disclosure of the security code to non-employees is strictly prohibited.
- The security code is changed on a periodic basis and eligible employees are notified by company e-mail or voice mail. Security codes are changed upon termination of employees that had access.
- The door to the reception area is locked at all times and requires appropriate credentials or escort past the reception or waiting area door(s).
- The reception area is staffed at all times during the working hours of 9:00 AM to 5:00 PM.
- Any unrecognized person in a restricted office location should be challenged as to their right to be there. All visitors must sign in at the front desk, wear a visitor badge, and be accompanied by a ARG staff member. In some situations, non-ARG personnel, who have signed the confidentiality agreement, do not need to be accompanied at all times.
- The building has motion detection sensors that are activated after hours. Any movement within the building will result in immediate notification to the police department.
- Fire Protection: Manufacturer's recommendations on the fire protection of individual hardware will be followed. There is a fire detection system installed within the office premises.

8 Telecommuting

With the increased availability of broadband access and VPNs, telecommuting has become more viable for many organizations. ARG considers telecommuting to be an acceptable work arrangement in certain circumstances. This policy is applicable to all employees and contractors who work either permanently or only occasionally outside of ARG office environment. It applies to users who work from their home full time, to employees on temporary travel, to users who work from a remote office location, and to any user who connects to ARG network and/or hosted EHR, if applicable, from a remote location.

While telecommuting can be an advantage for users and for the organization in general, it presents new risks in the areas of confidentiality and security of data. Workers linked to ARG's network become an extension of the wide area network and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. This arrangement also exposes the corporate data to risks not present in the traditional work environment.

8.1 General Requirements

Telecommuting workers are required to follow all corporate, security, confidentiality, HR, or Code of Conduct policies that are applicable to other employees/contractors.

- **Need to Know:** Telecommuting Users will have the access based on the same 'need to know' as they have when in the office.
- **Password Use:** The use of a strong password, is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.
- **Training:** Personnel who telecommute must complete the same annual privacy training as all other employees.
- **Contract Specific:** There may be additional requirements specific to the individual contracts to which an employee is assigned.

8.2 Required Equipment

ARG Provided:

ARG supplied workstation.
If printing, a ARG supplied printer.
If approved by your supervisor, a ARG supplied phone.
Broadband connection and fees,
Paper shredder,
Secure office environment isolated from visitors and family,
A lockable file cabinet or safe to secure documents when away from the home office.

8.3 Hardware Security Protections

Virus Protection**:** Home users must never stop the update process for Virus Protection. Virus Protection software is installed on all ARG personal computers and is set to update the virus pattern on a daily basis. This update is critical to the security of all data, and must be allowed to complete.

VPN and Firewall Use**:** Established procedures must be rigidly followed when accessing ARG information of any type. ARG requires the use of VPN software and a firewall device. Disabling a virus scanner or firewall is reason for termination.

Security Locks: Use security cable locks for laptops at all times, even if at home or at the office. Cable locks have been demonstrated as effective in thwarting robberies.

Lock Screens**:** No matter what location, always lock the screen before walking away from the workstation. The data on the screen may contain confidential information. Be sure the automatic lock feature has been set to automatically turn on after 10 minutes of inactivity.

8.4 Data Security Protection

Data Backup**:** Backup procedures have been established that encrypt the data being moved to an external media. Use only that procedure – do not create one on your own. If there is not a backup procedure established, or if you have external media that is not encrypted, contact the appropriate ARG personnel for assistance. Protect external media by keeping it in your possession when traveling.

Transferring Data to ARG**:** Transferring of data to ARG requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your own method, when transferring data to ARG.

External System Access: If you require access to an external system, contact your supervisor or department head. Privacy Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail: Do not send any individual-identifiable information (PHI or PII) via e-mail unless it is encrypted. If you need assistance with this, contact the Privacy Officer or appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

Non-ARG Networks: Extreme care must be taken when connecting ARG equipment to a home or hotel network. Although ARG actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, ARG has no ability to monitor or control the security procedures on non-ARG networks.

Protect Data in Your Possession: View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of data is kept at a minimum and that old data is eliminated as soon as possible. Store electronic data only in encrypted work spaces. If your laptop has not been set up with an encrypted work space, contact the Privacy Officer or appropriate personnel for assistance.

Hard Copy Reports or Work Papers: Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

Data Entry When in a Public Location: Do not perform work tasks which require the use of sensitive corporate level information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

Sending Data Outside ARG**:** All external transfer of data must be associated with an official contract, non-discloser agreement, or appropriate Business Associate Agreement. Do not give or transfer any information to anyone outside ARG without the written approval of your supervisor.

8.5 Disposal of Paper and/or External Media

Shredding: All paper which contains sensitive information that is no longer needed must be shredded before being disposed. Do not place in a trash container without first shredding. All employees working from home, or other non-ARG work environment, MUST have direct access to a shredder.

Disposal of Electronic Media: All external media must be sanitized or destroyed in accordance with compliant procedures.

- Do not throw any media containing sensitive, protected information in the trash.
- Return all external media to your supervisor
- External media must be wiped clean of all data. The Privacy Officer or appropriate personnel has very definitive procedures for doing this – so all external media must be sent to them.
- The final step in this process is to forward the media for disposal by a certified destruction agency.

9 Specific Protocols and Devices

9.1 Wireless Usage Standards and Policy

Due to an emergence of wireless access points in hotels, airports, and in homes, it has become imperative that a Wireless Usage policy be developed and adopted to ensure the security and functionality of such connections for ARG employees. This policy outlines the processes and procedures for acquiring wireless access privileges, utilizing wireless access, and ensuring the security of ARG laptops and mobile devices.

Approval Procedure **-** In order to be granted the ability to utilize the wireless network interface on your ARG laptop or mobile device you will be required to gain the approval of your immediate supervisor or department head and the Privacy Officer or appropriate personnel of ARG.

Software Requirements **-** The following is a list of minimum software requirements for any ARG laptop that is granted the privilege to use wireless access:

- Windows 7 Professional (Firewall enabled)
- Antivirus software
- Appropriate VPN Client, if applicable
- Internet Explorer 6.0 SP2 or Greater

If your laptop does not have all of these software components, please notify your supervisor or department head so these components can be installed.

Training Requirements **-** Once you have gained approval for wireless access on your ARG computer, you will be required to attend a usage and security training session to be provided by the Privacy Officer or appropriate personnel. This training session will cover the basics of connecting to wireless networks, securing your computer when connected to a wireless network, and the proper method for disconnecting from wireless networks. This training will be conducted within a reasonable period of time once wireless access approval has been granted, and in most cases will include several individuals at once.

9.2 Use of Transportable Media

Transportable media included within the scope of this policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, and USB key devices.

The purpose of this policy is to guide employees/contractors of ARG in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from ARG networks. Every workstation or server that has been used by either ARG employees or contractors is presumed to have sensitive information stored on its hard drive. Therefore procedures must be carefully followed when copying data to or from transportable media to protect sensitive ARG data. Since transportable media, by their very design are easily lost, care and protection of these devices must be addressed. Since it is very likely that transportable media will be provided to a ARG employee by an external source for the exchange of information, it is necessary that all employees have guidance in the appropriate use of media from other companies.

The use of transportable media in various formats is common ARG within ARG. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of ARG networks. Transportable media received from an external source could potentially pose a threat to ARG networks. ***Sensitive data*** includes all human resource data, financial data, ARG proprietary information, and secure information

USB key devices are handy devices which allow the transfer of data in an easy to carry format. They provide a much improved format for data transfer when compared to previous media formats, like diskettes, CD-ROMs, or DVDs. The software drivers necessary to utilize a USB key are normally included within the device and install automatically when connected. They now come in a rugged titanium format which connects to any key ring. These factors make them easy to use and to carry, but unfortunately easy to lose.

Rules governing the use of transportable media include:

- No ***sensitive data*** should ever be stored on transportable media unless the data is maintained in an encrypted format.
- All USB keys used to store ARG data or sensitive data must be an encrypted USB key issued by the Privacy Officer or appropriate personnel. The use of a personal USB key is strictly prohibited.
- Users must never connect their transportable media to a workstation that is not issued by ARG.
- Non-ARG workstations and laptops may not have the same security protection standards required by ARG, and accordingly virus patterns could potentially be transferred from the non-ARG device to the media and then back to ARG workstation.

Example: Do not copy a work spreadsheet to your USB key and take it home to work on your home PC.

- Data may be exchanged between ARG workstations/networks and workstations used within ARG. The very nature of data exchange requires that under certain situations data be exchanged in this manner.

Examples of necessary data exchange include:

Data provided to auditors via USB key during the course of the audit.

- It is permissible to connect transferable media from other businesses or individuals into ARG workstations or servers as long as the source of the media in on ARG Approved Supplier
- Before initial use and before any ***sensitive data*** may be transferred to transportable media, the media must be sent to the Privacy Officer or appropriate personnel to ensure appropriate and approved encryption is used. Copy ***sensitive data*** only to the encrypted space on the media. Non-sensitive data may be transferred to the non-encrypted space on the media.
- Report all loss of transportable media to your supervisor or department head. It is important that the CST team is notified either directly from the employee or contractor or by the supervisor or department head immediately.
- When an employee leaves ARG, all transportable media in their possession must be returned to the Privacy Officer or appropriate personnel for data deletion

ARG utilizes an approved method of encrypted data to ensure that all data is converted to a format that cannot be decrypted. The Privacy Officer or appropriate personnel can quickly establish an encrypted partition on your transportable media.

When no longer in productive use, all ARG laptops, workstation, or servers must be wiped of data in a manner which conforms to regulations. All transportable media must be wiped according to the same standards. Thus all transportable media must be returned to the Privacy Officer or appropriate personnel for data erasure when no longer in use.

10 Disposal of External Media / Hardware

10.1 Disposal of External Media

It must be assumed that any external media in the possession of an employee is likely to contain either secure or other sensitive information. Accordingly, external media (CD-ROMs, DVDs, diskettes, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be shredded and to utilize this policy in its destruction.
- External media should never be thrown in the trash.
- When no longer needed all forms of external media are to be sent to the Privacy Officer or appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used based on NIST 800-88 guidelines.

10.2 Requirements Regarding Equipment

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

10.3 Disposition of Excess Equipment

As the older ARG computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

- Older machines are regularly utilized for spare parts.
- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.
- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.
- Older machines are used to provide a second machine for personnel who often work from home.

11 Change Management

Statement of Policy

To ensure that ARG is tracking changes to networks, systems, and workstations including software releases and software vulnerability patching in information systems that contain secure information. Change tracking allows the Information Technology ("IT") Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

Procedure

1. The IT staff or other designated ARG employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system.
    a. When changes are tracked within a system, i.e. Windows updates in the Add or Remove Programs component, they do not need to be logged on the change management tracking log; however, the employee implementing the change will ensure that the change tracking is available for review if necessary.
2. The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
3. The employee implementing the change shall also be familiar with the rollback process in the event that the change causes an adverse effect within the system and needs to be removed.

12 Audit Controls

Statement of Policy

To ensure that ARG implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain electronic h information. Audit Controls are technical mechanisms that track and record computer activities. An audit trail determines if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or user activities.

ARG is committed to routinely auditing users' activities in order to continually assess potential risks and vulnerabilities in its possession. As such, ARG will continually assess potential risks and vulnerabilities to information in its possession and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with regulations.

Procedure

1. The Information Technology Services shall enable event auditing on all computers that process, transmit, and/or store secure information for purposes of generating audit logs. Each audit log shall include, at a minimum: user ID, login time and date, and scope of data being accessed for each attempted access. Audit trails shall be stored on a separate computer system to minimize the impact of such auditing on business operations and to minimize access to audit trails.

2. ARG shall utilize appropriate network-based and host-based intrusion detection systems. The Information Technology Services shall be responsible for installing, maintaining, and updating such systems.

13 Data Integrity

Statement of Policy

ARG shall implement and maintain appropriate electronic mechanisms to corroborate that secure information has not been altered or destroyed in an unauthorized manner.

The purpose of this policy is to protect ARG's secure information from improper alteration or destruction.

Procedure

To the fullest extent possible, ARG shall utilize applications with built-in intelligence that automatically checks for human errors.

ARG shall acquire appropriate network-based and host-based intrusion detection systems. The CM shall be responsible for installing, maintaining, and updating such systems.

To prevent transmission errors as data passes from one computer to another, ARG will use encryption, as determined to be appropriate, to preserve the integrity of data.

ARG will check for possible duplication of data in its computer systems to prevent poor data integration between different computer systems.

To prevent programming or software bugs, ARG will test its information systems for accuracy and functionality before it starts to use them. ARG will update its systems when IT vendors release fixes to address known bugs or problems.

1. ARG will install and regularly update antivirus software on all workstations to detect and prevent malicious code from altering or destroying data.
2. To prevent exposing magnetic media to a strong magnetic field, workforce members shall keep magnetic media away from strong magnetic fields and heat. For example, computers should not be left in automobiles during the summer months.

14 Contingency Plan

Statement of Policy

To establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain secure information.

ARG is committed to maintaining formal practices for responding to an emergency or other occurrence that damages systems containing secure. ARG shall continually assess potential risks and vulnerabilities to protect secure information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures.

Procedure

1. Data Backup Plan

    a. ARG, under the direction of the CM, shall implement a data backup plan to create and maintain retrievable exact copies of secure information.

    b. At the conclusion of each day, Monday through Friday, an incremental backup of all servers containing secure information shall be backed up to tape. On Saturday, a full backup of all servers containing secure information shall be backed up to tape. The backup tapes are taken each week off site by the IS Manager or his/her designee to ensure safeguard of ARG's data. One month of backup data will be maintained at all times in a remote location. Backup media that is no longer in service will be disposed of in accordance with the Disposal of External Media/Hardware policy.

    c. The CM shall monitor storage and removal of backups and ensure all applicable access controls are enforced.

    d. The CM shall test backup procedures on an annual basis to ensure that exact copies of secure information can be retrieved and made available. Such testing shall be documented by the CM. To the extent such testing indicates need for improvement in backup procedures, the CM shall identify and implement such improvements in a timely manner.

2. Disaster Recovery and Emergency Mode Operations Plan

    a. The CM shall be responsible for developing and regularly updating the written disaster recovery and emergency mode operations plan for the purpose of:

        i. Restoring or recovering any loss of secure information and/or systems necessary to make secure information available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and

        ii. Continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan shall be maintained on-site and at the off-site locations at which backups are stored or other secure off-site location.

    b. The disaster recovery and emergency mode operation plan shall include the following:

i. Current copies of the information systems inventory and network configuration developed and updated as part of ARG's risk analysis.

ii. Current copy of the written backup procedures developed and updated pursuant to this policy.

iii. Identification of an emergency response team. Members of such team shall be responsible for the following:

1. Determining the impact of a disaster and/or system unavailability on ARG's operations.

2. In the event of a disaster, securing the site and providing ongoing physical security.

3. Retrieving lost data.

4. Identifying and implementing appropriate "work-arounds" during such time information systems are unavailable.

5. Taking such steps necessary to restore operations.

iv. Procedures for responding to loss of electronic data including, but not limited to retrieval and loading of backup data or methods for recreating data should backup data be unavailable. The procedures should identify the order in which data is to be restored based on the criticality analysis performed as part of ARG's risk analysis

v. Telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster, including the following:

1. Members of the immediate response team,

2. Facilities at which backup data is stored,

3. Information systems vendors, and

4. All current workforce members.

c. The disaster recovery team shall meet on at least an annual basis to:

i. Review the effectiveness of the plan in responding to any disaster or emergency experienced by ARG;

ii. In the absence of any such disaster or emergency, plan drills to test the effectiveness of the plan and evaluate the results of such drills; and

iii. Review the written disaster recovery and emergency mode operations plan and make appropriate changes to the plan. The CM shall be responsible for convening and maintaining minutes of such meetings. The CM also shall be responsible for revising the plan based on the recommendations of the disaster recovery team.

15 Sanction Policy

Policy
It is the policy of ARG that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. ARG will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization.
ARG will take appropriate disciplinary action against employees, contractors, or any individuals who violate ARG's information security and privacy policies or confidentiality laws or regulations.

Purpose
To ensure that there are appropriate sanctions that will be applied to workforce members who violate the requirements ARG's security policies, Directives, and/or any other regulatory requirements.

Definitions
Workforce member means employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.
Sensitive information, includes, but not limited to, the following:

- Personnel files – Any information related to the hiring and/or employment of any individual who is or was employed by ARG.
- Payroll data – Any information related to the compensation of an individual during that individuals' employment with ARG.
- Financial/accounting records – Any records related to the accounting ARGs or financial statements of ARG.
- Other information that is confidential – Any other information that is sensitive in nature or considered to be confidential.

Availability refers to data or information is accessible and useable upon demand by an authorized person.
Confidentiality refers to data or information is not made available or disclosed to unauthorized persons or processes.
Integrity refers to data or information that have not been altered or destroyed in an unauthorized manner.

Violations
Listed below are the types of violations that require sanctions to be applied. They are stated at levels 1, 2, and 3 depending on the seriousness of the violation.

Level	Description of Violation
1	• Accessing information that you do not need to know to do your job. • Sharing computer access codes (user name & password). • Leaving computer unattended while being able to access sensitive information. • Disclosing sensitive information with unauthorized persons. • Copying sensitive information without authorization. • Changing sensitive information without authorization. • Discussing sensitive information in a public area or in an area where the public could overhear the conversation. • Discussing sensitive information with an unauthorized person. • Failing/refusing to cooperate with the

Level	Description of Violation
	Information MD or CM, and/or authorized designee.
2	• Second occurrence of any Level 1 offense (does not have to be the same offense). • Unauthorized use or disclosure of sensitive information. • Using another person's computer access code (user name & password). • Failing/refusing to comply with a remediation resolution or recommendation.
3	• Third occurrence of any Level 1 offense (does not have to be the same offense). • Second occurrence of any Level 2 offense (does not have to be the same offense). • Obtaining sensitive information under false pretenses. • Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.

Recommended Disciplinary Actions
In the event that a workforce member violates ARG's privacy and security policies) or related laws governing the protection of sensitive and identifiable information, the following recommended disciplinary actions will apply.

Violation Level	Recommended Disciplinary Action
1	• Verbal or written reprimand • Retraining on privacy/security awareness • Retraining on ARG's privacy and security policies • Retraining on the proper use of internal or required forms
2	• Letter of Reprimand*; or suspension • Retraining on privacy/security awareness • Retraining on ARG's privacy and security policies • Retraining on the proper use of internal or required forms
3	• Termination of employment or contract • Civil penalties as provided under applicable law

Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. If formal discipline is deemed necessary, ARG shall consult with Human Resources prior to taking action. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behavior which caused the disciplinary action.

*A Letter of Reprimand must be reviewed by Human Resources before given to the employee.

Exceptions
Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contract with ARG.

16 Employee Background Checks

ARG will conduct employment reference checks, investigative consumer reports, and background investigations on all candidates for employment prior to making a final offer of employment, and may use a third party to conduct these background checks.

An investigative consumer report compiles information on a candidate's general reputation and or personal characteristics. This information may be gathered online including social networking sites, through public or educational records, or through interviews with previous employers. In the pre-employment process, investigative consumer reports typically include such things as criminal records checks, education verification checks, and employment verification checks.

This information may also be sought out at other times during employment, such as during reassignment or promotional periods, and following safety infractions or other incidents.

ARG will conduct background checks in compliance with regulations. Applicants and employees may request and receive a copy of findings if requested.

A reported criminal offense conviction will not necessarily disqualify a candidate from employment. The nature and seriousness of the offense, the date of the offense, the surrounding circumstances, rehabilitation, the relevance of the offense to the specific position(s), and whether hiring, transferring or promoting the applicant would pose an unreasonable risk to the business may be considered before a final decision is reached.

ARG reserves the right to withdraw any offer of employment or consideration for employment, or discharge an employee, upon finding falsification, misrepresentation, or omission of fact on an employment application, resume, or other attachments, as well as in verbal statements, regardless of when it is discovered.
Background check reports shall be maintained in separate, confidential files and retained in accordance with ARG's document retention procedures.

Adapted from ***Carole Edman*** *of* ***HR Manager To Go Consultants*** *(http://www.amof.info/sample-policy.htm)*.

17 e-Discovery Policy: Retention

Policy
It is the policy of this organization to maintain and retain secure information and records in compliance with applicable governmental and regulatory requirements. This organization will adhere to retention schedules and destruction procedures in compliance with regulatory, business, and legal requirements.

Purpose
The purpose of this policy is to achieve a complete and accurate accounting of all relevant records within the organization; to establish the conditions and time periods for which paper based and electronic secure information and records will be stored, retained, and destroyed after they are no longer active for business purposes; and to ensure appropriate availability of inactive records.

Scope
This policy applies to all secure information and records whether the information is paper based or electronic. It applies to any secure record.

Definitions
Data Owners: Each department or unit that maintains secure information, either in electronic or paper form, is required to designate a records management coordinator who will ensure that records in his or her area are preserved, maintained, and retained in compliance with records management policies and retention schedules established.
Property Rights: No employee, by virtue of his or her position, has any personal or property right to such records even though he or she may have developed or compiled them.
Workforce Responsibility: All employees and agents are responsible for ensuring that secure information and records are created, used, maintained, preserved, and destroyed in accordance with this policy.
Unauthorized Destruction: The unauthorized destruction, removal, alteration, or use of secure information and records is prohibited. Persons who destroy, remove, alter or use secure information and records in an unauthorized manner will be disciplined in accordance with the organization's Sanction Policy.

Procedure

Responsible	Action
Data Owner/Departments	Data owners/departments will designate records coordinator for their areas and report that designation to the Records Committee and Litigation Response Team.
Record Committee	The record committee's role is to authorize any changes to the Retention, Storage, and Destruction policies and procedures; review and approve retention schedules and revisions to current retention schedules; address compliance audit findings; and review and approve control forms relating to business records.

Responsible	Action
CM	CM will convene the Record Committee as needed *[or at regular intervals]* and maintain responsibility for the following: • Review, maintain, publish, and distribute retention schedules and records management policies. • Audit compliance with records management (both electronic and paper) policies and retention schedules and report findings to Record Committee. • Serve as point of contact for Records Coordinators. • Provide training for Records Coordinators. Training will be provided on an individual basis to Records Coordinators and any individual or department that needs assistance. • Oversee operation of designated offsite record storage center(s) for archival storage of paper secure information and records or serve as contract administrator for such services. • Contract for destruction of paper and electronic records and certification thereof.
IT/Data Owners	IT/Data Owners will ensure that electronic storage of secure information and records is carried out in conjunction with archiving and retention policies.
Records Coordinators	Records coordinators are responsible for implementing and maintaining records management programs for their designated areas. They will organize and manage online records management control forms relating to enterprise records and information in their areas of responsibility to accomplish the following: • Transfer records to storage • Identify, control, and maintain records in storage • Retrieve and/or return records from/to storage • Document the destruction of records and the deletion of records from the records inventory • Monitor the records management process Record coordinators will obtain (if not already trained) and maintain records management skills.
Legal Services	Legal Services serves as subject matter expert and provides counsel regarding records designations and legal and statutory requirements for records retention and pending legal matters. It ensures that access to or ownership of records is appropriately protected in all divestitures of property or lines of business or facility closures.

Guidelines for Retention of Records/Information and Schedules:

Record Retention	Unless otherwise stipulated, retention schedules apply to all records. Records will only be discarded when the maximum specified retention period has expired, the record is approved for destruction by the record owner, and a Certificate of Destruction is executed.
Non-record Retention	Non-records are maintained for as long as administratively needed, and retention schedules do not apply. Non-records may and should be discarded when the business use has terminated. For example, when the non-record information, such as an employee's personal notes, is transferred to a record, such as an incident report, the notes are no longer useful and should be discarded. Preliminary working papers and superseded drafts should be discarded, particularly after subsequent versions are finalized. Instances where an author or recipient of a document is unsure whether a document is a record as covered or described in this policy should be referred to the Compliance Officer for determination of its status and retention period.
E-mail Communication Retention	Depending on content, e-mail messages between staff and clients and between clients and staff and documents transmitted by e-mail may be considered records and are subject to this policy. If an e-mail message would be considered a record based on its content, the retention period for that e-mail message would be the same for similar content in any other format. The originator/sender of the e-mail message (or the recipient of a message if the sender is outside Organization) is the person responsible for retaining the message if that message is considered a record. Users must save e-mail messages in a manner consistent with departmental procedures for retaining other information of similar content. Users should be aware of *Messaging Policies* that establish disposal schedules for e-mail and manage their e-mail accordingly.

Storage and Destruction Guidelines

Active/Inactive Records	Records are to be reviewed periodically by the Data Owner to determine if they are in the active, inactive, or destruction stage. Records that are no longer active will be stored in the designated off-site storage facility. Active stage is that period when reference is frequent and immediate access is important. Records should be retained in the office or close to the users. Data Owners, through their Records Coordinator, are responsible for maintaining the records in an orderly, secure, and auditable manner throughout this phase of the record life-cycle.
Active/Inactive Records, continued	Inactive stage is that period when records are retained for occasional reference and for legal reasons. Inactive records for which scheduled retention periods have not expired or records scheduled for permanent retention will be cataloged and moved to the designated off-site storage facility. Destruction stage is that period after records have served their full purpose, their mandated retention period, and finally are no longer needed.
Storage of Inactive Records	All inactive records identified for storage will be delivered with the appropriate Records Management Forms to the designated off-site storage facility where the records will be protected, stored, and will remain accessible and cataloged for easy retrieval. Except for emergencies, the designated off-site storage facility will provide access to records during normal business hours.

Records Destruction	General Rule: Records that have satisfied their legal, fiscal, administrative, and archival requirements may be destroyed in accordance with the Records Retention Schedules. Permanent Records: Records that cannot be destroyed include records of matters in litigation or records with a permanent retention. In the event of a lawsuit or government investigation, the applicable records that are not permanent cannot be destroyed until the lawsuit or investigation has been finalized. Once the litigation/investigation has been finalized, the record may be destroyed in accordance with the Records Retention Schedules but in no case shall records used in evidence to litigation be destroyed earlier than a specified number of years from the date of the settlement of litigation. Destruction of Records Containing Confidential Information: Records must be destroyed in a manner that ensures the confidentiality of the records and renders the information unrecognizable. A Certificate of Destruction form must be approved and signed by the appropriate management staff prior to the destruction of records. The Certificate of Destruction shall be retained by the off-site storage facility manager. Destruction of Non-Records Containing Confidential Information: Destruction Non-Records containing personal information or other forms of confidential corporate, employee, member, or information of any kind shall be rendered unrecognizable for both source and content by means of shredding, pulping, etc., regardless of media. This material shall be deposited in on-site, locked shred collection bins or boxed, sealed, and marked for destruction. Disposal of Electronic Storage Media: Electronic storage media must be assumed to contain confidential or other sensitive information and must not leave the possession of the organization until confirmation that the media is unreadable or until the media is physically destroyed.
Records Destruction, continued	Disposal of Electronic Media: Electronic storage media, such as CD-ROMS, DVDs, tapes, tape reels, USB thumb drives, disk drives or floppy disks containing confidential or sensitive information may only be disposed of by approved destruction methods.. CD-ROMs, DVDs, magneto-optical cartridges and other storage media that do not use traditional magnetic recording approaches must be physically destroyed. Disposal of IT Assets: Department managers must coordinate with the IT Department on disposing surplus property that is no longer needed for business activities according to the Disposal of IT Assets Policy. Disposal of information system equipment, including the irreversible removal of information and software, must occur in accordance with approved procedures and will be coordinated by IT personnel.