Apollo Education Group

Information Security

Asset Management Responsibility and Acceptable Use

Standards Document

13 December 2012
Version 1.8

TABLE OF CONTENTS

1 PURPOSE 3

2 SCOPE 3

3 ASSET MANAGEMENT - STANDARD STATEMENTS 3

4 ENFORCEMENT AND EXCEPTIONS 6

5 DEFINITIONS 7

6 REFERENCE DOCUMENTS 8

7 REVISION LOG 8

1 Purpose

The purpose of the Asset Management Standard is to ensure Apollo Education Group and all Apollo workers are protected from illegal and/or harmful actions that result from inappropriate use of Apollo Education Group systems, and to ensure that all Apollo workers are aware of their responsibilities for the proper use of Apollo assets.

2 Scope

2.1 This Standard applies to Apollo Education Group and each of its corporate affiliates, subsidiaries, owners, directors officers, agents and assignees (collectively referred to herein as Company or Apollo Education Group)

2.2 This Standard applies to all Apollo Education Group employees and others working on behalf of Apollo Education Group in a similar capacity including contractors, consultants, temporary workers, student placements etc. (known collectively throughout as -workers‖);

2.3 All Apollo Education Group information systems and all Apollo Education Group Intellectual Property (IP) within these systems, including backup copies, are the property of Apollo Education Group. See Intellectual Property Policy posted in the Corporate Policy Library. Policy Library

2.4 Any and all information stored on Apollo Education Group owned assets is subject to the Acceptable Use Standard. Workers will use all such resources in a manner that protects the security and privacy of Apollo Education Group Intellectual Property and will not engage in any activity that could endanger the security of information on Apollo Education Group assets.

3 Asset Management - Standard Statements

3.1 Responsibility for assets

3.1.1 It is the responsibility of every worker to protect Company assets from theft, destruction, or misuse. The following are key requirements related to these asset management responsibilities:

- Obtain manager approval prior to acquisition of all assets.
- Coordinate through Strategic Sourcing the acquisition of technology products pursuant to any new or existing contract with a provider of technology products and services. Purchase of non-standard assets requires detailed business justification.
- Purchase products that meet Company requirements as listed on the Strategic Sourcing Web Site. Strategic Sourcing

3.1.2 The Company retains the right to redistribute, refurbish, reconfigure or otherwise recondition any equipment for future use within the Company. Prior to retiring any assets you must contact Apollo Distribution for direction on appropriate methods to dispose of or retire assets.

3.1.3 Prior to the redistribution or retirement of an information system asset, you must coordinate with Campus System Administrators or IT Desktop Support personnel on the appropriate process to re-assign or retire the assets, and to ensure the asset is appropriately sanitized. (See Information Security Policy - Media Handling policy 10.7)

3.2 Acceptable Usage of Assets

3.2.1 Apollo Group assets are to be used in a professional, lawful and ethical manner consistent with the Code of Business Ethics. (See link)

3.2.2 It is against Apollo Education Group policy to install or run software without a valid license.

3.2.3 Apollo Education Group has identified, documented and implemented rules for the acceptable use of Company Assets. Company Assets must not be used for activities which have been identified as unacceptable conduct by the Company (see below)

Examples of unacceptable usage include (without limitation):

3.2.4 Workers will not use Apollo Education Group assets or resources to violate copyright or other laws through inappropriate reproduction and/or distribution (e.g., peer to peer file sharing) of music, movies, computer software, text, images, etc.

See – Intellectual Property Policy

3.2.5 Workers will not use Company assets to access, display or disseminate inappropriate information such as sexually explicit or racially or ethnically offensive materials. Failure to adhere to guidelines will result in disciplinary action up to and including termination.

3.2.6 Workers will not connect, plug in and/or load non-Company assets to the Company administrative network, including but not limited to, software, data storage devices, desktop computers and laptops. Campus System Technologists and members of Technical Support will not provide technical support for personal assets or products which are not listed as standards on the Strategic Sourcing Website. (See 3.1.1)

3.2.7 Other than when using Employee Mail Access Services (EMAS), workers will not use non-Apollo assets to conduct or communicate Apollo business. This includes the use of personal email and other personal communication mechanisms.

3.2.8 Workers will not access, download or transfer information, including but not limited to personally identifiable information, non-public financial information, or otherwise privileged or sensitive information, without explicit management approval.

3.2.9 Workers will not illegally duplicate, reproduce or share computer software.

3.2.10 Workers will not use Apollo Education Group assets or resources to engage in or promote activities such as hacking, gambling, terrorist activities, activities related to illegal weapons, or any other activity prohibited by law, rule or regulation.

3.2.11 Workers will not use Apollo Education Group assets or resources to access sites that:

- Are illegal, unethical or violate compliance or regulatory requirements
- Create a conflict of interest
- Contain inappropriate material for the work place
- Attempt to circumvent established controls

3.2.12 Workers will not use Apollo Education Group assets or resources to store and/or use any personal software or data, including, but not limited to, games and music files.

3.2.13 Unauthorized workers will not obtain passwords, encryption keys, or any other access control mechanisms that could permit unauthorized access to information or systems.

3.2.14 Consistent with the Social Networking Policy (link), workers will not use Apollo Education Group assets or resources to participate in non-business communications through the following methods:

- Social Networks
- Instant Messaging and Chat
- Discussion boards
- Newsgroups

3.2.15 Workers will not attempt to gain unauthorized access to information systems or information or in any way damaging, altering, or disrupting the operation of these systems, or use Company information systems as a staging ground or platform to gain unauthorized access to any other system or information.

3.2.16 Workers will not use tools such as network sniffers, password crackers or any other tools commonly associated with hacking except in the performance of assigned duties (e.g., members of the Apollo Education Group IT networking teams may use network sniffers to troubleshoot issues with the network).

3.2.17 Workers will not misrepresent, obscure, suppress or replace another worker's identity on information systems.

3.2.18 Workers will not associate unapproved domain name sites with a Company owned IP address.

3.2.19 Workers will not knowingly or carelessly perform an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.

3.2.20 Workers will not use Company resources for a personal or non-Apollo commercial activity, such as creating products or services for sale.

3.2.21 Workers will not use Apollo communication systems to harass or threaten others, or to send materials that might be deemed inappropriate, derogatory, prejudicial, or offensive. This includes sending repeated, unwanted e-mail to another worker.

3.2.22 Workers will not initiate, propagate or perpetuate electronic chain letters.

3.2.23 Workers will not send inappropriate mass mailings not directly associated with, or in the performance of, the routine course of duties or assignments. This includes multiple mailings to newsgroups, mailing lists, or individuals, e.g. "spamming."

3.2.24 Workers will not attempt to monitor or tamper with another worker's electronic communications, or read, copy, change, or delete another worker's files or software without the explicit agreement of the owner.

3.2.25 Workers will not authorize anyone to use their computer accounts for any reason, and are responsible for all use of their accounts. Workers must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of their account by unauthorized persons. Workers must not, for example, share passwords with anyone.

4 Enforcement and Exceptions

4.1 The Company reserves the right to monitor, access, retrieve, read, and disclose all messages created, sent, received, or stored on its assets (including connections made and sites visited), without prior notice.

4.2 Individuals that do not adequately protect assets may be subject to disciplinary action up to and including termination.

4.3 The Company reserves the right to automate technical policy enforcement where practical.

4.4 If workers are found to be in violation of the Asset Management policy and standards, the Company reserves the right to revoke access to and use of Apollo Education Group assets and services at any time, without notice, at its sole discretion.

4.5 The Company monitors, filters, and restricts internet activities. These measures are periodically updated and may change without notice at anytime. Exceptions to the standard filtering rules require management justification and approval.

4.6 Workers should be aware that when navigating through the Internet, they may be moving from an area of controlled access into an area of unknown security and information controls. Innocuous search requests may lead to offensive, sexually explicit and inappropriate materials. Worker accessing the Internet using Company resources do so at their own risk and the Company is not responsible for materials viewed or downloaded from the Internet.

4.7 Workers must report any violation of these regulations by another individual and any information relating to a flaw or bypass of Information Security policies or standards, to infosec@apollogrp.edu .

4.8 The Apollo Education Group Information Security Policy, along with supporting ITS Standards, are in place to assist the company in complying with legislative and regulatory requirements. Compliance is a task for everyone, including every employee, contractor, consultant, and

third party vendor. In certain specific circumstances it may not be feasible to comply with a policy or standards requirement. In such cases, it is critical to document each instance of non-compliance by filing an exception with the owner of the policy or standard and receiving approval. Security Exception Requests can be logged here: Link

4.9 At time of termination, or upon request by the Company, workers are to relinquish all assets, including information stored on Company-owned computer systems in an unencrypted, non-password protected and readily accessible form. Workers will not continue to access any Company computing or network resources after termination.

5 Definitions

- **Access control -** Security control designed to permit authorized access to an information system Administrative network—Company network that houses internal applications (3.2.13)
- **Backup -** A secondary copy of data on a separate form of media, e.g., tape media, remote disk storage system, CD-ROM, DVD, etc. (2)
- **Company asset -** Any product or service produced, provided or owned by Apollo Education Group and/or any of its subsidiaries
- **Electronic communications systems -** Media used to transfer information electronically, including Internet, voice mail, electronic mail, instant messages, posts to social network sights and fax
- **Encryption key -** Unique, secret data block used to encrypt data
- **Information system -** System consisting of the network of all communication channels used within an organization including operating systems, infrastructure, business applications, services, etc.
- **Internet -** External sites available to personnel who have a network connection
- **IP address -** An Internet Protocol address that is assigned to devices participating in a computer network
- **Mass communication -** Any marketing campaign using e-mail or mail where the recipients are leads that belong to multiple individuals
- **Media -** Various devices on which data is stored—tape, hard disk, diskette, CDROM, etc.
- **MP3 -** MPEG-1 Audio Layer 3, a de facto standard of digital audio compression for the transfer and playback of music on digital audio players
- **Password cracking -** Using software to guess at a password or try to re-create a password using a dictionary of predefined words
- **Workers –** Inclusive term used to describe employees, managers, custodians, contractors and all others who utilize Apollo Education Group information systems

6 Reference Documents

Other documents that are referred to or are associated with this document.

Document	Section	URL
Policies: Information Security Policy	Section 7	
Standards:		
Procedures:		

7 Revision Log

Author	Date	Description	Reviewer	Approver	Version
Bill Smathers	7/14/2010	Initial Creation	IT Security	Compliance	1.0
Bill Smathers	2/24/2011	Revised per Legal & AEC	IT Security	Compliance	1.7
Bill Smathers	12/13/2012	Reclassified as Public	IT Security	Compliance	1.8