



Apollo Group, Inc. – Information Security

Third Party Information Security Standards

Release Date: December 13, 2010

©2010 Apollo Group, Inc. All Rights reserved. No part of this document may be reproduced in any form without prior written permission from Apollo Group, Inc.

University of Phoenix®, Institute for Professional Development®, College for Financial Planning®, and Western International University ® are registered trademarks of Apollo Group, Inc.

TABLE OF CONTENTS

1	PURPOSE	4
2	SCOPE	4
3	STANDARD STATEMENTS	4
3.1	REQUIREMENTS FOR ALL COMPANIES	4
3.1.1	INFORMATION SECURITY RISK MANAGEMENT	4
3.1.2	INFORMATION SECURITY POLICY	4
3.1.3	ORGANIZATION OF INFORMATION SECURITY	4
3.1.4	ASSET MANAGEMENT	5
3.1.5	HUMAN RESOURCES SECURITY	5
3.1.6	PHYSICAL AND ENVIRONMENTAL SECURITY	6
3.1.7	OPERATIONS MANAGEMENT	6
3.1.7.1	Network Security	6
3.1.7.2	System Security	6
3.1.7.3	Data Security	7
3.1.7.4	Operation Security	7
3.1.8	ACCESS CONTROL	7
3.1.9	INFORMATION TECHNOLOGY ACQUISITION, DEVELOPMENT AND MAINTENANCE	9
3.1.10	INFORMATION SECURITY INCIDENT MANAGEMENT	9
3.1.11	BUSINESS CONTINUITY MANAGEMENT	10
3.1.12	COMPLIANCE	10
3.2	ADDITIONAL REQUIREMENTS FOR HOSTING SERVICE PROVIDERS	11
3.2.1	OPERATIONS MANAGEMENT	11
3.2.1.1	Network Security	11
3.2.1.2	System Security	12
3.2.1.3	Data Security	12
3.2.1.4	Operations Security	12
3.2.2	ACCESS CONTROL	13
4	ENFORCEMENT AND EXCEPTIONS	13
5	DEFINITIONS	13
6	REVISION LOG	14

1 Purpose

The purpose of this standard is to establish information security requirements for Companies that perform services for Apollo or otherwise have access to Apollo Assets.

2 Scope

If a Company has access to Apollo Assets, Company must handle, treat, and otherwise protect Apollo Assets in accordance with all requirements, policies, standards, processes and procedures set forth in this policy and any contractual agreement between such Company and Apollo. If there is a direct conflict between any term of this policy and the terms of a written contract between Company and Apollo, the terms of the written contract will prevail to the extent of the conflict.

3 Standard Statements

3.1 Requirements for all Companies

3.1.1 Information Security Risk Management

- a. Companies must periodically assess risk within Information Technology (“IT”) that accesses Apollo Assets.

3.1.2 Information Security Policy

- a. Companies must have a documented and followed Information Security program that is based on at least one of the following Information Technology industry leading security frameworks of;
 - i. International Organization for Standardization (“ISO”) 27002,
 - ii. Information Security Forum (“ISF”) Standards of Good Practice (“SoGP”), or
 - iii. National Institute of Standards and Technology (“NIST”) Special Security Publications.
- b. Companies must map their security program to one of the above security frameworks. Maps must not show any gaps in Company security programs.

3.1.3 Organization of Information Security

- a. Companies must define, document and assign ownership to oversee development, adoption, enforcement and compliance with Information Security requirements, policies, standards and procedures.
- b. Companies must ensure the assigned role must be of a sufficiently high-level classification in the organization that can be allowed to execute the responsibilities in an effective and independent manner.
- c. To avoid conflicts of interest, Companies must ensure this role will not have direct responsibility for information processing and technology operations.

3.1.4 Asset Management

- a. Companies must have a managed and up-to-date inventory of Company's Assets that access Apollo Assets.
- b. Company must assign designated individual that is responsible for all Company Assets that access Apollo Assets.
- c. Companies must document and implement rules for the acceptable use of Assets of third parties, including without limitation, Apollo Assets.
 - i. Rules of acceptable use must require that third party Assets are not be used for activities which have been identified as unacceptable conduct.
 - ii. Rules of acceptable use must require that third party Assets are to be used in a professional, lawful and ethical manner.
- d. All Companies who connect to or use an Apollo Asset (including servers, workstations, infrastructure, internet gateway or network) must abide by all applicable Apollo terms of use, standards and procedures, and any supporting standards and procedures. Companies are required to safeguard and use Apollo Assets wisely and will use good judgment and discretion when using Apollo Assets including Apollo systems, computers, telephones, Internet access, email, voice mail, copiers, fax machines, vehicles or other property.
- e. Companies must never connect non-Apollo owned Assets to the Apollo network without direct written approval from Apollo.
 - i. Apollo must review and approve of all requests from any Company to connect non-Apollo owned Assets to the Apollo network.
 - ii. Assets that connect to Apollo network must abide by Apollo security standards, operating practices and controls including, but not limited to configuration, hardening, patching, access control and virus protection processes.

3.1.5 Human Resources Security

- a. Companies must ensure all Company employees and Company subcontractors who access Apollo Assets are screened prior to employment. Screening must include criminal, financial, employment background screening processes.
- b. Company must have processes in place to periodically screen personnel during employment for anyone who accesses Regulated, Confidential or Personal Information.
- c. Companies must ensure an Information Security awareness campaign is provided to anyone who access Apollo Assets. Campaign must educate personnel of their responsibility to secure Apollo Assets.
- d. Companies must ensure all User IDs, tokens or physical-access badges are assigned to a unique Company employee or Company subcontractor.

- e. Companies must ensure all user/system/service/administrator accounts and passwords are never shared.
- f. Companies must immediately notify Apollo in writing if a Company employee or Company subcontractor with access to Apollo Assets terminates, is not working on the Apollo account or ID permission must be changed on an Apollo managed technology. Notices must include name, User ID name of any accounts the person had access to or knows the password.

3.1.6 Physical and Environmental Security

- a. Company must store Apollo Assets in locations that are protected from;
 - i. Natural disasters,
 - ii. Theft, physical intrusion, unlawful and unauthorized physical access, and
 - iii. Ventilation, Heat or Cooling problems, Power failures or outages.

3.1.7 Operations Management

3.1.7.1 Network Security

- a. Companies must deploy Data Leakage Prevention (“DLP”) and or Intrusion Monitoring Services at perimeter points where Apollo Regulated, Confidential or Personal Information is used.
- b. Companies must ensure all unnecessary services, ports and network traffic are disabled on all IT systems that access Apollo Assets.

3.1.7.2 System Security

- a. Companies must have a process for applying and managing security updates, patches, fixes, upgrades, (collectively referred to as “Patches”) on all Company IT systems.
 - i. Companies must ensure Patches that provide security fixes or security updates are deployed in 30 days from a manufacture’s release on all IT systems that access Confidential, Personal or Regulated Information.
 - ii. Otherwise, Companies must ensure Patches that provide security fixes or security updates are deployed within 120 days from a manufacturer release on all IT systems that access Apollo Assets.
- b. Company must ensure Malware, Virus, Trojan and Spyware protection is deployed on all IT systems that access Apollo Assets.
- c. Company must ensure Malware, Virus, Trojan and Spyware protection technology have the latest and up-to-date manufacture’s signatures, definition files, software and patches.
- d. Companies must deploy Host Intrusion and Prevention Systems (“HIPS”) and software firewalls on all Company IT systems that access Apollo Assets.
 - i. HIPS and software firewalls must have the latest and up-to-date manufacture’s signatures, definition files, software patches.
 - ii. Software firewalls must be configured to monitor and block unauthorized traffic.

- iii. HIPS must be configured to monitor and block threats and unauthorized software.
 - iv. HIPS and Software firewalls must be configured to report all unauthorized activity to a secure central repository that retains records for up to one year.
 - v. If requested by Apollo, Company must provide logs of all unauthorized activity captured in HIPS, software firewalls and any other log files.
- e. Companies must ensure all unused or unnecessary software, applications, services, sample/default files and folders are disabled on all IT systems that access Apollo Assets.

3.1.7.3 Data Security

- a. Company must use strong encryption key management practices to ensure the availability of encrypted authoritative information.
- b. Companies must encrypt all Apollo Assets in transmission between Company and Apollo and between Company and all external sources. External sources includes Apollo's business partners and subcontracting companies and Company's business partners and subcontracting companies
- c. Companies must encrypt Regulated Information at rest at all times.
- d. Encryption must meet minimal standards of 168 bit encryption

3.1.7.4 Operation Security

- a. Companies must ensure that any changes to IT systems that are performing work on or for do not have any negative security implications.
- b. Companies must follow documented change management procedures
- c. Companies must not move or transfer Regulated, Personal or Confidential Information to any non-production environment or insecure location.

3.1.8 Access Control

- a. Companies must ensure controls restrict other Company customers from accessing Apollo Assets.
- b. Companies must use authentication and authorization technologies for service, user and administrator level accounts.
- c. Companies must not allow Apollo or Company employees or subcontractors direct root access to any systems or access to the administrator user account.
 - i. For Unix or Unix-like Operating systems, users must use the "sudo" command where all access must be logged.
- d. Companies must ensure IT administrators are provided and using separate and unique administrator accounts that are only used for administration responsibilities. Non-administration tasks must always be performed using non-administrator user accounts.

- e. Companies must ensure password policies and standards exist on IT systems that access Apollo Assets.
- f. Companies must ensure systems that access Confidential, Personal or Regulated Information require the following password construction requirements at all times;
 - i. Minimum length: 8 characters
 - ii. Complexity: Must contain at least three of the following four characters: Number, Uppercase letter, Lowercase letter, Printable special character
 - iii. History (reuse): ≥ 10 passwords
 - iv. Expiration: ≤ 90 days – including system administrators
 - v. Service account passwords must be changed at least annually
 - vi. Failed login attempts: ≤ 6 attempts
 - vii. Account lockout: ≥ 30 minutes
 - viii. Screen saver locks must be enabled: ≤ 15 minutes for OS and ≤ 30 minutes for applications containing sensitive information
- g. Companies must ensure systems that access Apollo Assets meet the following additional requirements at all times;
 - i. Authentication credentials must be encrypted when stored or transmitted at all times
 - ii. Passwords for user-level accounts cannot be shared between multiple individuals
 - iii. Companies must change their passwords immediately whenever it is believed that an account may have been compromised.
 - iv. Passwords must not be communicated via email messages or other forms of electronic communication, other than one-time use passwords.
 - v. Passwords for individual user accounts must never be given to or shared with someone other than the account owner
 - vi. A user's identity must be verified before their password is reset and an email or voicemail notification must be sent to notify the user that their password was reset.
 - vii. First-time passwords for new user accounts must be set to unique values that follow the requirements set forth in this standard and must not be generic, easily-guessed passwords.
 - viii. User accounts must be configured to force a change of their password upon first use of a new account or after a password is reset.
 - ix. All manufacturer passwords must be changed from their default values (including when the default value is NULL) and must meet the requirements set forth in this standard. manufacturer passwords include, but are not limited to, SNMP community strings, system-level administrator account passwords, temporary account passwords, wireless encryption keys, and other default authentication settings.
 - x. Password fields must display only masked characters as the user types in their password, where technically feasible.
 - xi. Hardcode plain-text passwords must not be used in production environments.
 - xii. Production account passwords must not be used in non-production environments.
 - xiii. If a system-level administrator account (e.g. Windows local administrator or UNIX/Linux root) is used to perform privileged management of a device, that password must be changed following completion of that management task.

- xiv. If an account has a machine-set complex password of 20 characters or more that is never accessed or known by a human, that password does not need to be changed during its lifetime, unless the account or its associated system has been suspected of compromise.
 - xv. System-level account passwords must be unique on each device.
 - xvi. Service-level accounts may be set to never lock out due to failed login attempts and do not need to enforce password expiration.
 - xvii. All systems must prompt users to re-authenticate when users attempt to elevate their privileges to higher security levels. Examples include use of sudo or su on UNIX/LINUX systems or “run as” for Microsoft Windows based systems.
- h. Companies must ensure procedures exist for prompt modification or termination of access or rights in response to organizational changes.
 - i. Companies must ensure procedures exist for provisioning privileged accounts.
 - j. Companies must periodically review the necessity of privileged access accounts
 - k. If Company requires remote access to Apollo’s Assets, Companies must always use an Apollo approved method to remotely connect to any Apollo Asset.
 - i. Companies must never install technology that provides remote access to any Asset on the Apollo network including, but not limited to; analog phone line remote access technologies (e.g. modems), Virtual Private Networks, Remote access software, etc.

3.1.9 Information Technology Acquisition, Development and Maintenance

- a. Companies must ensure Infrastructure, network and application vulnerability assessments are periodically conducted and follow industry acceptable vulnerability management practices (e.g. processes described in NIST & OWASP)
- b. Companies must ensure industry acceptable application development security standards (e.g. OWASP) are followed so that IT systems and applications are tested and secured in every step of the application and system development life cycle.
- c. Companies must ensure firmware, software and application source code are validated and tested against vulnerabilities and weaknesses before deploying to production.

3.1.10 Information Security Incident Management

- a. Companies must ensure access and activity audit and logging procedures, including access attempts and privileged access, exist.
- b. Companies must ensure security incident response planning and notification procedures exist to monitor, react, notify and investigate any incident related to an Apollo Assets.
- c. Companies must immediately notify Apollo if Company identifies a breach in any controls that impacts an Apollo Asset or data related to an Apollo Asset.

- d. Once Companies discover or are notified of a security breach, Companies must investigate, fix, restore and conduct a root cause analysis.
- e. Companies must provide Apollo with results and frequent status update of any investigation related to Apollo.
- f. If Apollo is not satisfied with speed or effectiveness of investigation, Companies must include Apollo Information Security staff in the investigation and response teams.

3.1.11 Business Continuity Management

- a. When required by Apollo, Company and Apollo must document and agree to an achievable and tested Recovery Time Objectives (“RTOs”)
- b. Company must maintain a comprehensive and current; Business Continuity Plan (“BCP”) that documents processes and procedures that are implemented to ensure essential business functions continue to operate during and after a disaster; and Disaster Recovery Plan (“DRP”) that documents technical plans for specific restoration of Apollo processes and Assets .
- c. BCP and DRP must be updated after function, process or IT changes.
- d. BCP and DRP must be tested on a frequent basis.
- e. If requested by Apollo, summary and detailed results of DRP and BCP tests must be provided to Apollo.

3.1.12 Compliance

- a. Data destruction processes must follow a process that securely wipes all data on all media using a method that will not allow data to be retrieved. For all IT systems that access Regulated, Confidential, or Personal Information, Apollo requires the destruction be performed in accordance with NIST Special report 800-88, Gutmann Method, US DoD 5220-22.M
- b. If requested by Apollo, Company must provide adequate validation of any subcontracted company is compliant with this document.
- c. Company must obtain written permission from the Apollo Legal Department to move Apollo Assets across any international borders.
- d. Companies must secure all Credit Card data in accordance to requirements listed in the most current and released editions of the Payment Card Industry – Data Security Standards (“PCI-DSS” or “PCI”).
- e. Companies that access Credit Card data must annually provide evidence of PCI certification/compliance.

3.2 Additional requirements for Hosting Service Providers

In addition to all requirements listed above, the following requirements must be followed by all Companies who provide hosting services to Apollo. Hosted services include, without limitation, cloud computing or offsite hosting services. Cloud computing can be Company service offerings that allow Apollo to dynamically lease and provision Infrastructure, Virtual Environments, Platforms and Software.

Companies that provide hosting services are responsible for all requirements below.

In the event the Company's hosting service model shifts some responsibility of the below requirements to Apollo, the Company must still complete a "Policy Exception Request" as defined in Section 4 of this document to clearly define ownership or responsibility. Apollo will not assume any ownership for any requirement below without a direct agreement listed in a written contract, statement of work or an Apollo approved Policy Exception Request.

3.2.1 Operations Management

- a. Companies who provide Infrastructure and Platform hosting services must ensure Non-Apollo authorized personnel cannot physically or electronically inspect, insert, share, access, steal or change content of Apollo Assets, including without limitation Apollo used network, traffic, infrastructure, applications, RAM and storage space.

3.2.1.1 Network Security

- a. Within Apollo used or leased services, Companies must restrict by protocol, service port and source IP address, and MAC address through the use of firewall technologies.
- b. Companies must ensure firewalls are configured with different policies that allow Apollo used Web Servers, Application Servers and databases are protected with different levels of security.
 - i. Companies must ensure network segmentation and firewall restrictions exist so that Apollo used database servers can only communicate with the following; Application servers located in an Application Virtual Local Area Networks (VLANs), Management Tool Servers located in Management Tool VLANs, and Network Administration Users located in Admin VLANs.
 - ii. Companies must ensure network segmentation and firewall restrictions exist so that Apollo used Application servers can only communicate with the following; Web servers located in Web VLANs, databases located in database VLANs, Management Tool Servers located in Management Tool VLANs, and Network Administration Users located in Admin VLANs.
- c. Companies must use additional security protection controls for protecting against access to Apollo Regulated, Personal, or Confidential Information, such as; Web Application Firewalls, Intrusion Detections Systems, Intrusion Prevention Systems and Data Loss Prevent Systems.
- d. Companies must ensure Web Server, App Servers and databases administrative functions are only accessed via SSH or a secure method that encrypts traffic during transmission.

3.2.1.2 System Security

- a. Companies must ensure Apollo Assets reside on separate physical hardware from other service provider customers including data distributed in different environments (e.g. backup media, production, development, test, quality assurance, disaster recovery) when transferring or storing Apollo Regulated, Personal, or Confidential Information.
- b. For services that leverage Virtual Environments (“VE”), Companies must ensure VE’s;
 - i. Use Apollo standard builds or Apollo approved builds,
 - ii. Company provided platform, build, standard image, or related template for guest operating systems, are validated by Apollo to ensure security requirements are correctly integrated.
 - iii. OS patches are easily deployable to all un-patched servers and applications so that all servers can comply with Apollo Patch management standards.
 - iv. VE specific security mechanisms embedded in hypervisor APIs are utilized to provide granular monitoring of traffic crossing VE backplanes, which will be opaque to traditional network security controls.
 - v. Administrative access and control of VE operating systems include strong authentication integrated with enterprise identity management, as well as tamper-proof logging and integrity monitoring tools.
 - vi. Are segregated in security zones by type of usage (e.g., desktop vs. server), production stage (e.g., development, production, and testing) and sensitivity of data (e.g. Apollo Regulated data) on separate physical hardware components such as servers, storage, etc.
 - vii. Have a reporting mechanism in place that provides evidence of VE isolation and raises alerts if there is a breach of isolation.
 - viii. Have capability for File Integrity Monitoring (FIM) to be deployed on VEs to alert on critical file changes.
- c. Companies must configure and filter inbound and outbound traffic per instance using host-based firewalls.

3.2.1.3 Data Security

- a. Company must encrypt data at rest and in transit in accordance to all regulatory bodies (e.g. PCI), local and national laws (examples are, but are not limited to the following; HIPPA, SoX, GLBA, etc).
- b. Company must sign and encrypt API requests.

3.2.1.4 Operations Security

- a. Company must ensure that when objects are deleted, all mappings to the objects are also removed.
- b. Company must ensure that when domains, objects and trusts are deleted, all mappings to the domains, objects and trusts are also removed.
- c. Company must provide Apollo with the ability to monitor and review critical files for changes or tampering.

3.2.2 Access Control

- a. For systems that access Apollo classified Confidential, Personal or Regulated Information, Company must deploy and offer token or key-based authentication to improve authentication controls.

4 Enforcement and Exceptions

The Apollo Group Third Party Information Security Policy, are in place to assist Apollo in complying with best practices and legislative and regulatory requirements. Compliance is a task for everyone, including every employee, contractor, consultant, and Company. In certain specific circumstances it may not be feasible to comply with a policy or standards requirement. In such cases, it is critical to obtain prior approval of an exception to this policy. If Apollo approves the non-compliance, Company must document and maintain a record of such instance.

Specifically, If a Company can not comply with a requirement listed in this document, then Company must submit a Policy Exception Request and follow the Policy Exception Request process to gain written approval from Apollo's IT Services - Information Security Department. A Policy Exception Request can be completed by sending an email to Infosec@apollogrp.edu. If Company will be applying for a Policy Exception Request, a request must be submitted and approved before any services are provided to Apollo.

This document can be amended with or without notice from time to time in Apollo's sole and absolute discretion. Companies will need to frequently monitor this document for any changes. Companies will be expected to comply with any changes to this document.

5 Definitions

"Infosec" or **"Information Security Department"** is the specific department in Apollo's Information Technology Services ("ITS") division responsible for the governance of Apollo Information security policies, standards, procedures and processes.

The verb **"access"**, **"accessed"** or **"accessing"** is any one or a combination of the following actions: (i) To handle, (ii) To access, (iii) To process, (iv) To store, (v) To transmit, (vi) To touch, (vii) To view; (viii) To host.

"Company" for the purpose of this policy, Company will be defined as any non-Apollo owned entity that provides products or services to Apollo, including but not limited to third party service providers and suppliers.

"Asset" includes, but is not limited to: (i) information, such as data, databases, hosted data, computer files, documentation, manuals, plans and audit logs; (ii) software, such as application and system software; and (iii) physical equipment, such as computer hardware, peripheral devices and communication.

"Apollo" (or **"Apollo Group, Inc."**) with its principal place of business at 4025 S. Riverpoint Parkway, Phoenix, AZ 85040. Apollo includes Apollo affiliates and subsidiaries and their respective subsidiaries.

“Regulated Information” is Personal Information or Confidential Information that requires the greatest degree of controls and safeguards to ensure compliance with state, federal or international law, rule, regulation or ordinance. Examples include, but are not limited to; Credit Card information, Debit Card information, Bank Account information, Social Security Number, Student Records, Protected Health Information, etc.

“Confidential Information” means all confidential and proprietary information of Apollo and includes Personal Information.

“Personal Information” means any information that Company obtains in any manner from any source during or in connection with its performance of services for Apollo that concerns any of Apollo prospective, former and existing students, customers or employees. Personal Information includes, without limitation, names, addresses, telephone numbers, e-mail addresses, social security numbers, credit card numbers, call-detail information, student records, purchase information, product and service usage information, account information, credit information, demographic and any other personally identifiable information.

6 Revision Log

Document review and revision tracking

Author	Date	Description	Reviewer	Approver	Version
Information Security	12/13/2010	Released Edition	Information Security	Information Security	1.0