Apollo Education Group
Information Security

Third Party Information Security Standards

Document Type: Standard

Document Serial No. [TBD per applicable matrix]
Original Release: 12/13/2010

SME / Author Review – Reboot File	
SME Reviewer:	B. Smathers, M. Hernandez
Review Date:	SME/Author Initials:
Approval Date:	SME/Author Initials:

File Title	Third Party Information Security Standards
Author	A. Charad
Release Date	08/26/2015
Source Document	Apollo-Education-Group-IT-Policies-Third-Party.pdf http://www.apollo.edu/sites/default/files/files/Apollo-Group-IT-Policies-Third-Party.pdf

Compliance	6.2 External Parties

Revision Log

Author	Date	Description of Change	Reviewed By	Approval By	Revision Number
Information Security	12/13/2010	Released Edition	Information Security	Information Security	1.0
C. Cupone	08/06/2013	Revision and Update	C. Cupone	B. Smathers	2.0
A. Charad	08/26/2015	Revision and Update	M. Hernandez	B. Smathers	3.0

Document Change Control Notice

This document can be amended with or without notice from time to time in Apollo's sole and absolute discretion. Companies will not be expected to comply with any changes to this document until they have been provided with such changes in writing and a reasonable period (not to exceed 120 days) to comply with such changes.

Since it incorporates formal statements of Apollo Education Group policy, this document is subject to a strict change control process. Notes are published on the intranet when major updates to this manual are published and, if appropriate, emails are circulated to relevant parties notifying them of the changes.

Feedback comments, corrections and improvement suggestions on this policy manual (including any areas that are not sufficiently well covered) are welcome from any part of Apollo Education Group at any time. VendorRiskManagement@apollo.edu

Proposed alterations to the manual will be analyzed and developed by Information Security in conjunction with relevant subject matter experts (SME). Updates may be circulated for comment, clearly labeled as DRAFTs. DRAFTs are not intended for implementation and do not necessarily reflect official Apollo Education Group policy until they are formally approved and posted by the Corporate Policy Governance Committee.

The manual as a whole must also be comprehensively reviewed by the VP of Information Security and updated as necessary every year. The Corporate Policy Governance Committee must review and re-approve the policy statements at least once every two years.

TABLE OF CONTENTS

1. Purpose

Presented within this document are information security requirements, policies, and standards for vendor companies that render services to Apollo Education Group and/or have access to Apollo Education Group Assets.

2. Scope

This standard establishes guidelines, practices, and requirements for vendor companies are responsible while providing services to Apollo Education Group. Subject matter includes: Requirements for all Companies, Organization of Information Security, Asset Management, Human Resources Security, Operations Management, Access Control, among others security subjects.

3. Executive Summary

This document presents guidelines and practices regarding Vendor Company IT Security. Included are Apollo Education Group and Vendor Company interactions regarding responsibilities, risk and asset management, human resources security, requirements, policies, and standards relevant to Information Security.

4. Responsibility

4.1 Content Accuracy

GRC, Legal Department

4.2 Implementation

GRC, Strategic Sourcing and Procurement Departments

4.3 Primary Users

Strategic Sourcing and Procurement Departments, Vendor Companies, Sub-contractor employees, and/or any Apollo-approved agent who renders contractual services to the enterprise

Return to TOC

5. Third-Party Information Security Standards

Overview

1. **General requirements for Companies having access to Apollo Assets**

   If a Company has access to Apollo Assets, that 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.

2. **Resolving conflict between policy terms and written contract terms**

   If there is a direct conflict between any term of this policy and the terms of a written contract between Company and Apollo Education Group, the terms of the written contract will prevail to the extent of the conflict.

5.1 Requirements for all Companies

5.1.1 Information Security Risk Management

Companies must periodically assess risk within Information Technology ("IT") that accesses Apollo Assets.

5.1.2 Information Security Policy

1. **Security Program requirements**

   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, such as:

   A. International Organization for Standardization ("ISO") 27001

   B. Information Security Forum ("ISF") Standards of Good Practice ("SoGP"), or,

   C. National Institute of Standards and Technology ("NIST") Special Security Publications

2. **Security Program framework**

   Companies must map their security program to one of the above security frameworks. Maps must not show any gaps in Company security programs.

5.1.3 Organization of Information Security

1. **Companies to define, document, assign oversight ownership**

   Companies must define, document and assign ownership to oversee development, adoption, enforcement and compliance with Information Security requirements, policies, standards and procedures.

Return to TOC

2. **Companies must assure effective execution of responsibilities**

   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.

3. **Companies must avoid conflict of interest**

   To avoid conflicts of interest, Companies must ensure this role will not have direct responsibility for information processing and technology operations.

5.1.4 Asset Management

1. **Managing up-to-date inventory of Company's Assets**

   Companies must have a managed and up-to-date inventory of Company's Assets that access Apollo Assets.

2. **Assigning designated individual regarding accessing Apollo Assets**

   A Company must assign a designated individual that is responsible for all Company Assets that access Apollo Assets.

3. **Documenting and implementing rules for acceptable use**

   Companies must document and implement rules for the acceptable use of Assets of third parties, including without limitation, Apollo Assets.

4. **Rules of acceptable use requirements**

   A. Rules of acceptable use must require that third party Assets are not to be used for activities which have been identified as unacceptable conduct.

   B. Rules of acceptable use must require that third party Assets are to be used in a professional, lawful and ethical manner.

5. **Companies connected to Apollo Assets must abide by terms of use**

   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 apply good judgment and discretion when using Apollo Assets including:

   - Apollo systems
   - voice mail
   - fax machines
   - computers
   - email
   - or other property
   - telephones
   - copiers
   - Internet access
   - vehicles

Return to TOC

6. **Written approval required for connection to non-Apollo Assets**

   Companies must never connect non-Apollo owned Assets to the Apollo network without direct written approval from Apollo.

   A. **Apollo reviews and approves requests for company connections to non-Apollo assets.**
   Apollo must review and approve of all requests from any Company to connect non-Apollo owned Assets to the Apollo network.

   B. **Standards regarding connecting to Apollo network**
   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
- Virus Protection processes

5.1.5 Human Resources Security

1. **Requirement for pre-employment screening**

   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.

2. **Screening employees who access Regulated, Confidential, Personal information**

   Company must have processes in place to periodically screen personnel during employment for anyone who accesses Regulated, Confidential or Personal Information.

3. **Ensuring Information Security awareness**

   Companies must ensure an Information Security awareness campaign is provided to anyone who accesses Apollo Assets. Company must educate personnel of their responsibilities to secure Apollo Assets.

4. **Assigning unique User IDs, tokens, physical-access badges**

   Companies must ensure all User IDs, tokens or physical-access badges are assigned to a unique Company employee or Company subcontractor.

5. **Disallowing the sharing of passwords regarding Apollo Assets**

   Companies must ensure all user/system/service/administrator accounts which have access to Apollo Assets and passwords are never shared.

6. **Notifying Apollo upon employee or sub-contractor termination**

   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.

Return to TOC

5.1.6 Physical and Environmental Security

Company must store Apollo Assets in locations that are protected from:

- Natural disasters
- Theft
- Physical intrusion
- Heat or Cooling problems
- Power failures or outages
- Ventilation
- Unlawful and unauthorized physical access

5.1.7 Operations Management

1. Network Security

A. **Data Leakage Prevention or Intrusion Monitoring Services**
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. **Disabling unnecessary services on IT systems that access Apollo Assets**
Companies must ensure all unnecessary services, ports and network traffic are disabled on all IT systems that access Apollo Assets.

2. System Security

A. **Company process for updates, patches, fixes, and upgrades**
Companies must have a process for applying and managing security updates, patches, fixes, upgrades, (collectively referred to as "Patches") on all Company IT systems.

- Companies must use Patches that provide security fixes or security updates are deployed in 30 days from a manufacturer's release on all IT systems that access Confidential, Personal, or Regulated Information.
- 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 ensuring Malware, Virus / Trojan / Spyware protection**
Companies must ensure Malware, Virus, Trojan and Spyware protection is deployed on all IT systems that access Apollo Assets.

C. **Company to have latest / up-dated protection technology**
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.

Return to TOC

D. **Companies to deploy Host Intrusion and Prevention Systems**
Companies must deploy Host Intrusion and Prevention Systems (“HIPS”) and software firewalls on all publically accessible Company IT systems that access Apollo Assets.

- HIPS and software firewalls must have the latest and up-to-date manufacture’s signatures, definition files, software patches.
- Software firewalls must be configured to monitor and block unauthorized traffic.
- HIPS must be configured to monitor and block threats and unauthorized software.
- 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.
- If requested by Apollo, Company must provide logs of all unauthorized activity captured in HIPS, software firewalls, and any other log files.

E. **Companies to disable unnecessary software / applications / services**
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. Data Security

A. **Companies to use strong encryption key management**
Company must use strong encryption key management practices to ensure the availability of encrypted authoritative information.

B. **Encrypting Apollo Assets in transmission between Company and external sources**
Companies must encrypt all Apollo Assets in transmission between Company and Apollo and between Company and all external sources.

External sources include Apollo's business partners and subcontracting companies and Companies’ 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.**

Return to TOC

4. **Operation Security**

   A. **Ensuring against negative security implications per IT Systems changes**
   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. **Restriction from moving / transferring information to non-production environment**
   Companies must not move or transfer Regulated, Personal or Confidential Information to any non-production environment or insecure location.

5.1.8 Access Control

1. **Restricting Company customers from accessing Apollo Assets**

   Companies must ensure controls restrict other Company customers from accessing Apollo Assets.

2. **Using authentication and authorization technologies**

   Companies must use authentication and authorization technologies for service, user and administrator level accounts.

3. **Restricting direct root access from Company employees or subcontractors**

   Companies must not allow Apollo or Company employees or subcontractors direct root access to any systems or access to the administrator user account.

   Note: For UNIX or UNIX-like Operating systems, users must use the "sudo” command where all access must be logged.

4. **Providing IT administrators unique accounts**

   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.

5. **Assuring password policies and standards regarding Apollo Assets**

   Companies must ensure password policies and standards exist on IT systems that access Apollo Assets.

6. **Password construction requirements**

   Companies must ensure systems that access Confidential, Personal or Regulated Information require the following password construction requirements at all times:

   A. Minimum length: 8 characters

   B. Complexity: Must contain at least three of the following four characters: Number, Uppercase letter, Lowercase letter, Printable special character

Return to TOC

C. History (reuse): >. 10 passwords

D. Expiration: <= 90 days — including system administrators

E. Service account passwords must be changed at least annually

F. Failed login attempts: <= 6 attempts

G. Account lockout: > 29 minutes

H. Screen saver locks must be enabled: <= 15 minutes for OS and <= 30 minutes for applications containing sensitive information

7. Additional requirements regarding systems that access Apollo Assets

Companies must ensure systems that access Apollo Assets meet the following additional requirements at all times:

A. Authentication credentials must be encrypted when stored or transmitted at all times

B. Passwords for user-level accounts cannot be shared between multiple individuals

C. Companies must change their passwords immediately whenever it is believed that an account may have been compromised.

D. Passwords must not be communicated via email messages or other forms of electronic communication, other than one-time use passwords.

E. Passwords for individual user accounts must never be given to, or shared with, someone other than the account owner.

F. 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 their password was reset.

G. 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.

H. 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.

I. 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.

J. Password fields must display only masked characters as the user types in their password, where technically feasible.

K. Hardcode plain-text passwords must not be used in production environments.

L. Production account passwords must not be used in non-production environments.

Return to TOC

M. 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.

N. 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.

O. System-level account passwords must be unique on each device.

P. Service-level accounts may be set to never lock out due to failed login attempts and do not need to enforce password expiration.

Q. 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.

8. Procedures for modification or termination of access rights

Companies must ensure procedures exist for prompt modification or termination of access or rights in response to organizational changes.

9. Procedures for provisioning privileged accounts

Companies must ensure procedures exist for provisioning privileged accounts.

10. Required periodic review of privileged access accounts

Companies must periodically review the necessity of privileged access accounts.

11. Provision for remote access to Apollo Assets

If a Company requires remote access to Apollo Assets, that Company must always use an Apollo approved method to remotely connect to any Apollo Asset.

12. Restriction against installing remote access technology to Apollo Assets

Companies must never install technology that provides remote access to any Asset on the Apollo network including, but not limited to:

A. Analog phone line remote access technologies (e.g. modems)

B. Virtual Private Networks

C. Remote access software, etc.

5.1.9 Information Technology Acquisition, Development and Maintenance

1. Companies to ensure periodic vulnerability assessments

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).

Return to TOC

2. **Ensuring industry-acceptable security standards**

   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.

3. **Ensuring firmware and software source code testing and validation**

   Companies must ensure firmware, software and application source code are validated and tested against vulnerabilities and weaknesses before deploying to production.

5.1.10 Information Security Incident Management

1. **Ensuring access and activity audit and logging procedures**

   Companies must ensure access and activity audit and logging procedures, including access attempts and privileged access, exist.

2. **Ensuring security incident response planning and notification procedures**

   Companies must ensure security incident response planning and notification procedures exist to monitor, react, notify and investigate any incident related to an Apollo Assets.

3. **Notifying Apollo when identifying a breach impacting Apollo Assets**

   Companies must notify Apollo, consistent with the requirements of the Master Agreement if Company identifies a breach in any controls that impacts an Apollo Asset or data related to an Apollo Asset.

4. **Companies must investigate, fix, restore, and perform root cause analysis**

   Once Companies discover or are notified of a security breach, Companies must investigate, fix, restore and conduct a root cause analysis.

5. **Providing results and status updates of investigations per Apollo Assets**

   Companies must provide Apollo with results and frequent status update of any investigation related to Apollo.

6. **Provision for Apollo Information Security staff to assist in investigations**

   If Apollo is not satisfied with speed or effectiveness of investigation, Companies must include Apollo Information Security staff in the investigation and response teams. Company will work with Apollo to address any concerns.

5.1.11 Business Continuity Management

1. **Recovery Time Objectives (RTOs) agreement**

   When required by Apollo, Company and Apollo must document and agree to an achievable and tested Recovery Time Objectives (RTOs).

Return to TOC

2. **Business Continuity Plan (BCP), Disaster Recovery Plan (DRP)**

   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 a Disaster Recovery Plan (“DRP”) that documents technical plans for specific restoration of Apollo processes and Assets according to published RTOs.

3. **BCP and DRP must be updated after function, process, or IT changes.**

4. **BCP and DRP must be tested on a frequent basis.**

5. **Providing Apollo with DRP and BCP summary results**

   If requested by Apollo, summary results of DRP and BCP tests must be provided to Apollo.

5.1.12 Compliance

1. **Data destruction processes**

   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

2. **Companies to provide validation of subcontractor companies**

   If requested by Apollo, Company must provide adequate validation of any subcontracted company is compliant with this document. Company is required to insure of any subcontracted company is compliant with this document.

3. **Obtaining permission to move Apollo Assets across international borders**

   Company must obtain written permission from the Apollo Legal Department to move Apollo Assets across any international borders.

4. **Companies to secure all credit card data per industry standards**

   If applicable to the services provided to Apollo, 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”).

5. **Annually, companies to provide evidence of PCI certification / compliance**

   If applicable to the services provided to Apollo, Companies that access Credit Card data must annually provide evidence of PCI certification/compliance.

Return to TOC

5.2 Additional requirements for Hosting Service Providers

Overview

A. **Additional requirements per hosting services and cloud computing**
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.

B. **When Implementing "Policy Exception Request"**
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 7** 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.

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

5.2.1 Operations Management

1. Company to ensure Apollo Asset protection

Companies who provide Infrastructure and Platform hosting services must ensure Non-Apollo authorized personnel cannot physically or electronically:

- Inspect
- Share
- Access
- Steal, or,
- Change content to:

Apollo Assets, including (without limitation):

- Apollo used network
- Traffic
- Infrastructure
- Applications
- RAM
- Storage space

2. Network Security

A. **Restricting protocol, service port, source IP Address, MAC Address**
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. **Ensuring firewalls configured to allow Apollo-used Web Servers**
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.

Return to TOC

- Companies must ensure network segmentation and firewall restrictions exist so that Apollo used database servers can only communicate with the following:
  1) Application servers located in an Application Virtual Local Area Networks (VLANs)
  2) Management Tool Servers located in Management Tool VLANs, and,
  3) Network Administration Users located in Admin VLANs
- Companies must ensure network segmentation and firewall restrictions exist so that Apollo used Application servers can only communicate with the following:
  1) Web servers located in Web VLANs
  2) Databases located in database VLANs
  3) Management Tool Servers located in Management Tool VLANs, and,
  4) Network Administration Users located in Admin VLANs

C. **Companies to provide additional security protections**
Companies must use additional security protection controls for protecting against access to Apollo Regulated, Personal, or Confidential Information, such as:

- Web Application Firewalls
- Intrusion Prevention Systems
- Intrusion Detection Systems
- Data Loss Prevent Systems

D. **Administrative functions accessed via SSH**
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. System Security

A. **Ensuring Apollo Assets reside on separate physical hardware**
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 that VEs:**

- Use Apollo standard builds or Apollo approved builds,
- Company provided platform, build, standard image, or related template for guest operating systems, are validated by Apollo to ensure security requirements are correctly integrated.

Return to TOC

- OS patches are easily deployable to all un-patched servers and applications so that all servers can comply with Apollo Patch management standards.
- 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.
- 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.
- 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.
- Have a reporting mechanism in place that provides evidence of VE isolation and raises alerts if there is a breach of isolation.
- Have capability for File Integrity Monitoring (FIM) to be deployed on VEs to alert on critical file changes.

C. **Configuring and filtering inbound / outbound traffic**
Companies must configure and filter inbound and outbound traffic per instance using host-based firewalls.

4. Data Security

A. **Encrypting data at rest / in transit**
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.**

5. Operations Security

A. **Deleting objects and all mappings**
Company must ensure that when objects are deleted, all mappings to the objects are also removed.

B. **Deleting domains, objects, trusts and all mappings**
Company must ensure that when domains, objects and trusts are deleted, all mappings to the domains, objects and trusts are also removed.

C. **Apollo to monitor and review critical files**
Company must provide Apollo with the ability to monitor and review critical files for changes or tampering.

Return to TOC

5.2.2 Access Control

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.

6. Definitions

Term	Definition
Asset	Includes, but is not limited to: 1. Information, such as data, databases, hosted data, computer files, documentation, manuals, plans and audit logs 2. Software, such as application and system software, and, 3. Physical equipment, such as computer hardware, peripheral devices and communication.
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 Vendors.
Confidential Information	All confidential and proprietary information of Apollo and includes Personal Information.
Infosec	“Information Security Department” - The specific department in Apollo’s Information Technology Services (ITS) division responsible for the governance of Apollo Information security policies, standards, procedures and processes.
ISF	“Information Security Forum” is an international, independent, non-profit organization dedicated to benchmarking and identifying good practice in information security.
ISO	“International Organization for Standardization” is an international-standard-setting body composed of representatives from various national standards organizations.
NDA	Non-Disclosure Agreement
NIST	“National Institute of Standards and Technology” is a measurement standards laboratory, which is a non-regulatory agency of the United States Department of Commerce.
OWASP	Open Web Application Security Project Return to TOC

Term	Definition
Personal Information	Any information that a 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.
Regulated Information	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.
SNMP	Simple Network Management Protocol - one of the primary protocols used to gather data about systems.
SRA	Vendor Risk Assessment
SSH	Secure Shell - Industry-standard protocol for securing communications.

7. Enforcement and Exceptions

Enforcement

The Apollo Education Group Third Party Information Security Policy and commensurate standards 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.

This document can be amended with or without notice from time to time in Apollo's sole and absolute discretion. Companies will not be expected to comply with any changes to this document until they have been provided with such changes in writing and a reasonable period (not to exceed 120 days) to comply with such changes.

Exceptions

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, the Company must document and maintain a record of such instance.

Return to TOC

Specifically, if a Company cannot comply with a requirement listed in this document, the sponsoring VP 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.

Return to TOC