Aspen Group, Inc. (AGI)

# **Approval and Ownership**

The **VP, Technology** is the authorized decision maker who can either approve or deny changes to this policy.

# **Revision History**

This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  **Version** | **Date of Change** | **Section** | **Description of Change** | **Change Authority** |
| 1.0 | 3/2019 | Full Document | Reformatting, Updates | Gerard Wendolowski |
|   |   |   |   |   |
|   |   |   |   |   |
|   |   |   |   |   |
|   |   |   |   |   |
|   |   |   |   |   |
|   |   |   |   |   |
|   |   |   |   |   |
|   |   |   |   |   |

# **Enforcement**

Any personnel found to have violated any policy shall be subject to disciplinary action, up to and including termination of employment.

**Table of Contents**

**1.0 Purpose Page 4**

**1.1 Scope Page 4**

**2.0 Roles & Responsibilities Page 4**

**3.0 Policies & Compliance Page 6**

 **3.0.1 Exceptions………. Page 6**

 **3.0.2 Auditability………. Page 6**

 **3.0.3 Modifications………. Page 6**

 **3.0.4 Inquiries………. Page 6**

**3.1 User Security Training………. Page 6**

**3.2 Passwords………. Page 7**

**3.3 External Connectivity………. Page 8**

**3.4 User Access Management………. Page 9**

**3.5 Virus Prevention………. Page 12**

**3.6 General Security………. Page 13**

**3.7 Server Security………. Page 13**

**3.8 Monitoring & Logging………. Page 16**

**3.9 Hardware………. Page 17**

**3.10 Internet Access………. Page 18**

**3.11 Communication………. Page 19**

**3.12 Physical Security………. Page 20**

**3.13 Application Security………. Page 22**

**3.14 Employee & Student Inquiries………. Page 24**

**3.15 Data Retention & Backups………. Page 24**

**1.0 Purpose**

The goal of the Information Security Manual is to appropriately manage the information security risk to the enterprise by creating and managing security policies.

Policies are security rule statements, identified and created by IT management as a method or means to achieve appropriate levels of protection. Standards are methodologies and technologies accepted by IT management for the enterprise. Identified standards within this manual must be followed.

**1.1 Scope**

The scope of the Information Security Manual covers all of the applications, systems; networks and data center facilities managed by IT. Users are defined as any associate, contractor, temporary associate or anyone else given access to applications, systems, and network or data center facilities.

**2.0 Roles & Responsibilities**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Enrollment Advisor | 1. Manage prospective student inquiries.
2. Assist prospective students in completing their application.
3. Gather required documentation, and store it in the document management system.
4. Assist accepted students with setting up their payment method and first course registration.
 |
| Academic Advisor | 1. Manage current student inquiries.
2. Troubleshoot student issues.
3. Support students with course registration.
4. Support students with the classroom technology.
 |
| Bursar | 1. Manage all aspects of student finances.
 |
| Financial Aid | 1. Manage all aspects of student finances for students utilizing Federal Student Aid as their payment method.
 |
| Finance (Corporate) | 1. Manage all aspects of the University’s finances.
2. Review student payments.
3. Retrieve data related to costs and revenue.
 |
| Technology  | 1. Support each institution’s technology needs.
2. Maintain and upgrade in-house software to meet the institution’s requirements.
3. Setup third party integrations.
4. Troubleshoot system errors.
 |
| Records Coordinator | 1. Manage student files and documents.
 |
| Registrar | 1. Manage student’s account.
2. Manage accepting students to the University.
 |

2.1 Employee Background Check

Policy: Employees of AGI’s Technology Team are required to complete a background check prior to their start date.

Exceptions: Prior to September 25th, 2018 employees hired at AGI (non-technology), Aspen University or United States University were not required to complete a background check.

Owner: VP, Human Resources

2.2 FERPA Policy

Policy: Employees of AGI and its subsidiaries are required to complete FERPA training within their first 12 months of employment. The Registrars at Aspen University and United States University maintain a record of each employee’s FERPA training.

Owner: Registrar

**3.0 Policy & Compliance**

No single policy or set of standards can cover all situations that affect information system security, in order to preserve information processing effectiveness, some exceptions may be necessary.

**3.0.1 Exceptions**

Exceptions will be considered by management on an individual basis.

**3.0.2 Auditability**

Management and designated auditors (internal and external) have the right to review, audit or observe all applications and data.

**3.0.3 Modifications**

The COO is the only one who can make modifications to this policy document. This document is reviewed annually, updated where appropriate and approved by the company’s Chief Financial Officer and Chief Executive Officer.

**3.0.4 Inquiries**

Any questions regarding information security policy should be directed to the Chief Operating Officer.

**3.1 User Security Training**

3.1.1 Security Awareness Training

Policy: The Technology Team is responsible for distributing security information to employees.

Commentary: The Senior IT Manager distributes security and policy information to employees.

Owner: Senior IT Manager

 3.1.2 Secure Code Training

Policy: The Technology Team’s developers are issued Veracode licenses and are given time to complete secure code training courses.

Commentary: The Veracode agreement was executed in March 2019, and licenses issued in April 2019.

Owner: VP, Technology

**3.2 Passwords**

 3.2.1 Password Length

Policy: Passwords are required to be a minimum of 8 characters.

Systems In Scope: CRM, Student Information System, VPN, Employee Workstation, Google Apps

 Owner: VP, Systems

3.2.2 Password Complexity

Policy: Password complexity is enabled. Password complexity requires at least one uppercase, one lowercase, one numeric and one special character.

Systems In Scope: CRM, Student Information System, VPN, Employee Workstation, Google Apps

 Owner: VP, Systems

3.2.3 Password Aging

Policy: Passwords must expire after 180 days.

Commentary: This policy limits the compromising of user passwords.

Systems In Scope: Student Information System

Exceptions: CRM, Student Portal, Application, Vendors

 Owner: VP, Systems

3.2.4 Sharing of User Accounts and Passwords

Policy: Individual accounts and passwords cannot be shared. Group or Generic accounts and shared passwords are explicitly prohibited. Accounts and passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the account.

Systems In Scope: CRM, Student Information System, Student Portal, Student Application

 Owner: Senior IT Manager

3.2.5 Passwords stored in an AGI database are not in a readable form

Policy: Passwords that are stored in an AGI database are encrypted.

Effective Date: March 2019

Owner: VP, Technology

3.2.6 Two Factor Authentication

Policy: Designated employee are required to have two-factor authentication in place to access their Google Apps account

Employees In Scope: Finance (Bursar, Financial Aid, Corporate), Technology (All employees), Executive (Officers, Vice Presidents)

Effective Date: March 1st, 2019

Owner: Senior IT Manager

3.2.7 Lock accounts after invalid login attempts

Policy: AGI has limited users to 5 invalid login attempts. After 5 unsuccessful attempts the user is required to reset their password via a link sent to their email.

Systems In Scope: Student Information System, Student Portal, CRM

Effective Dates:

Student Information System & Student Portal Effective March 15, 2019.

CRM Effective April 1, 2019.

 Owner: VP, Systems

**3.3 External Connectivity**

3.3.1 Two Factor Authentication for VPN Access

 Policy: All individuals connecting to the VPN are using two-factor authentication.

Commentary: The VPN connection requires the end point, name of the site and a key. After those have been authorized the end-user can enter their username and password.

Owner: VP, Systems

3.3.2 VPN Inactivity Timeout

 Policy: The VPN connection times out after 30 minutes of inactivity.

 Commentary: The timeout is managed by Rackspace.

Owner: VP, Systems

3.3.3 Transmitting Confidential Information

Policy: Any transaction that requires Confidential Information to be transmitted between AGI and a vendor, the transmission must use SSL, SFTP or VPN.

Commentary: SSL requires the use of advanced 128-bit or better SSL encryption technology to ensure confidential information cannot be viewed. Confidential Information is defined as a record containing Social Security Number.

Systems In Scope: Global Financial Aid Services Extract

Owner: VP, Technology

**3.4 User Access Management**

3.4.1 Access to data

Policy: AGI maintains a “least privileged” access philosophy for all users in regards to student and employee data. User access is restricted by only allowing access to systems based on the user’s role and responsibility.

Systems In Scope: CRM, Student Information System, Database Servers, Web Servers, VPN

Owner: VP, Technology

3.4.2 Uniquely identify students and employees

Policy: AGI grants a unique ID to each user that has access to a system.

Commentary: The purpose of this policy is to provide a unique identifier which allows the technology team to manage permissions, and identify activity for specific users.

Systems In Scope: CRM, Student Information System

Owner: VP, Technology

3.4.3 Manage Permissions

Policy: Applications have a module built into its system that supports granting, modifying or revoking permissions for specific user.

Commentary: The security or user management module allows the Technology Team to limit access to specific tools, data, reports etc..

Systems In Scope: CRM, Student Information System

Owners: VP, Technology

3.4.4 Identifying who has the ability to control user access.

Policy: AGI has identified specific, qualified employees that have control over user access.

 Systems In Scope: CRM, Student Information System

Employees: Senior IT Manager, IT Support Specialists, Application Support Analyst, VP of Systems, VP of Technology, Chief Operating Officer

Owner: VP, Technology

3.4.5 Tracking requests for system access.

Policy: The AGI Technology Team tracks all system access requests through ZenDesk.

Systems In Scope: CRM, Student Information System

Exceptions: When a user is migrated to a new system, they may inherit permissions similar to the previous system. Document access requests are handled at the University level. Users may be given access to systems, features or tools that fall within their job description without a Permissions Form.

Owner: VP, Systems

3.4.6 Granting access to systems.

Policy: The AGI Technology Team will grant an employee access to a specific system or feature upon receipt of a completed Permissions Form.

Commentary: The Permissions Form contains the details of the request and authorization from the employee’s manager.

Systems In Scope: CRM, Student Information System, Production Database Servers, Production Web Servers, VPN

Exceptions: When a user is migrated to a new system, they may inherit permissions similar to the previous system. Document access requests are handled at the University level. Users can be given access to systems, features or tools that fall within their job description without a Permissions Form.

 Owner: VP, Systems

3.4.7 VPN access is administered by the VP of Systems.

Policy: The VP of Systems is the only employee authorized to grant an employee access to the VPN.

Systems In Scope: VPN

 Owner: VP, Systems

3.4.8 Server access is administered by the VP of Systems

Policy: The VP of Systems is the only employees authorized to grant an employee access to a production database, or production web server.

Systems In Scope: Production Database Servers, Production Web Servers

Owners: VP, Systems

3.4.9 Revoking access to systems.

Policy: The AGI Technology Team will revoke an employee’s access to a specific system or feature upon receipt of a completed Permissions Form.

Commentary: The Permissions Form contains the details of the request and authorization from the employee’s manager.

Systems In Scope: Determined by the requestor.

Exceptions: In circumstances where access need to be revoked immediately, documentation will occur after access has been revoked.

Owner: VP, Systems

3.4.10 Terminated employees have their access revoked.

Policy: The AGI Technology Team will revoke an employee’s system access upon notification.

Commentary: In most cases the employee’s manager will submit a Permissions Form.

Systems In Scope: All systems owned or controlled by AGI.

Exceptions: In circumstances where access need to be revoked immediately, documentation will occur after access has been revoked.

Owner: VP, Systems

 3.4.11 Administrative access to work stations.

 Policy: Employees do not have administrative access to their work station.

 In Scope: Enrollment Advisors

 Exceptions: All non-Enrollment Advisors.

 Effective Date: April 30, 2019

 Owner: Senior IT Manager

**3.5 Virus Prevention**

 3.5.1 Workstation Virus Protection

Policy: AGI’s Technology Team establishes virus scanning for all software on desktop computer workstations.

 In Scope: Full-time employee work stations.

 Exceptions: Full-time employees designated as faculty, Consultants

 Owner: Senior IT Manager

3.5.2 Workstation Virus Definition Updates

Policy: Antivirus software is configured on each desktop computer workstation to automatically update antivirus definitions.

 In Scope: Full-time employee work stations.

 Exceptions: Full-time employees designated as faculty, Consultants

Owner: Senior IT Manager

**3.6 General Security**

3.6.1 Encrypting Passwords & Social Security Numbers

Policy: Passwords and Social Security Numbers that are stored in a database are encrypted using the AES/CBC/PKCS5Padding algorithm, which uses encryption keys to manage encryption.

Owner: VP, Technology

3.6.2 Credit Card Information must not be stored.

Policy: Credit card information is not stored in an AGI database.

Owner: VP, Technology

3.6.3 Security Incident Reporting

Policy: All suspected information security incidents must be promptly reported to the VP. Systems.

Commentary: This policy is intended to require that all problems and violations be promptly reported.

Owner: VP, Systems

3.6.4 Employees are not the administrators of their workstations.

Policy: AGI limits the employees that have administrative privileges of their workstations.

Commentary: A new control added during this audit review period for Enrollment Advisors.

In Scope: Enrollment Advisors

Effective Date: April 30, 2019

Owner: Senior IT Manager

**3.7 Server Security**

3.7.1 Server Configuration Practices

Policy: AGI’s Technology Team has implemented a Server Configuration Policy, and applied it to all of its Production Servers.

Commentary: This policy was created in April 2019, and all Production Servers were evaluated and brought into compliance with this policy.

Exceptions: USUGP & Tableau were not migrated from UTC to PST, but will be migrated during FY ‘20.

 In Scope: Production Database Servers, Production Web servers

 Owner: VP, Systems

3.7.2 Server Virus Protection

Policy: AGI’s Technology Team has virus scanning software enabled on all database and web servers.

 In Scope: Database servers, Web servers

 Effective Dates:

 USUGP: March 28, 2019

 Tableau: March 28, 2019

 Owner: VP, Systems

3.7.3 Server Virus Definition Updates

Policy: Antivirus software is configured on all database and web servers to automatically update antivirus definitions.

 In Scope: Database servers, Web servers

Owner: VP, Systems

3.7.4 Server Security Updates

Policy: The VP of Systems or Senior IT Manager review Security Update Notifications once per month, to determine which are applicable to AGI’s software. The VP of Systems and Senior IT Manager determine the severity of the security update and whether or not to apply the update to the server. All update are first deployed on a development server and actively monitored for a period of time (no less than 5 days, no more than 30 days) before a deployment is scheduled for production.

Commentary: This policy was updated on March 1, 2019 to include deployment to the development server, prior to production.

Effective Date: March 1, 2019

In Scope: Production Database Servers, Production Web Servers, USU’s Internal Network Server (Deactivated on March 7, 2019)

 Owner: VP, Systems

3.7.5 Servers are on an internal network and behind a firewall.

Policy: The database and web servers are on an internal network that is protected by a firewall.

 Owner: VP, Systems

3.7.6 Employees cannot physically access a server.

Policy: AGI employees cannot physically access servers because AGI uses third parties for all database and web server hosting.

Exceptions: USU’s Internal Network Server (Deactivated on March 7, 2019)

Owner: VP, Systems

**3.8 Monitoring & Logging**

3.8.1 Server Performance Logging

Policy: AGI utilizes a third party, PRTG Network Monitor, to monitor the performance of its production servers.

Commentary: The VP, Systems has configured PRTG Network Monitor to send email alerts when certain conditions are met. PRTG Monitoring was expanded from 9 to 24 servers during March 2019.

Owner: VP, Systems

3.8.2 Monitoring of Automated Processes

Policy: AGI utilizes a third party, PRTG Network Monitor, to monitor the result of a specific jobs or automated processes.

Commentary: The VP, Systems has configured PRTG Network Monitor specific SQL Schedule Jobs, Windows Schedule Tasks, Windows Services, CF Scheduled Jobs.

 In Scope: Mandrill, Quickbooks

Exceptions: The VP, Technology & VP, Systems determine which processes require PRTG Network Monitor. The Daily Billing Job is monitored through an email that is configured at the server level.

Owner: VP, Systems

3.8.3 Server Security Update Logging

Policy: The VP of Systems and Senior IT Manager maintain a log of all server security updates.

In Scope: Database servers, Web servers, USU’s Internal Network Server (Termination Date)

Owner: VP, Systems

3.8.4 System Access Review

Policy: The AGI Technology Team reviews access to specific systems on an annual basis to make sure that access is consistent with the individual’s role and responsibilities.

Systems In Scope: CRM, Student Information System, Database Servers, Web Servers, VPN, Critical Vendors

Exceptions:

Owner: COO

3.8.5 Physical Access Review

Policy: The AGI Technology team reviews access to each office on annual basis.

Owner: Senior IT Manager

3.8.6 Logging and Monitoring Security Violations

Policy: The AGI Technology Team defines invalid login attempts as a Security Violation. Security Violations are logged and reviewed once per month.

Systems in Scope: CRM, Student Information System, VPN

Effective Date: March 15, 2019

Owner: VP, Systems

**3.9 Hardware**

3.9.1 Maintain a Hardware Inventory

Policy: The Senior IT Manager maintains a hardware inventory.

Commentary: The hardware inventory is meant to support an occasional hardware failure, and to decrease the amount of downtime an employee experiences.

In Scope: Full-time employee work stations.

Owner: Senior IT Manager

3.9.2 Hardware Inventory Tracking

Policy: The Senior IT Manager maintains a detailed inventory list, by employee.

Commentary: The Senior IT Manager has identified all hardware that has been issued to employees.

In Scope: Full-time employee work stations.

Owner: Senior IT Manager

**3.10 Internet Access**

3.10.1 On-Site Internet Access Firewall

Policy: All internet access in company facilities must be routed through an authorized firewall.

Commentary: This policy prevents users from deliberately or unwittingly circumventing the controls supported by a firewall.

Owner: Senior IT Manager

3.10.2 Wireless Network equipment installations

Policy: Any wireless network installed in a company facility must be approved by the Senior IT Manager.

Exceptions: Approval may also be granted by the VP of Systems.

Owner: Senior IT Manager

3.10.3 Wireless Networks Encryption Security

Policy: All wireless networks are configured to employ WPA2 or similar encryption.

Commentary: This policy will strengthen wireless encryption and reduce the risk of hackers gaining unauthorized access to the wireless network.

Owner: Senior IT Manager

3.10.4 On-Site Wifi Internet Access

Policy: All internet access in company facilities using a Wifi connection requires a password administered by the Senior IT Manager.

Commentary: This policy prevents unauthorized users from accessing the Wifi network.

Owner: Senior IT Manager

**3.11 Communication**

3.11.1 Use of Company Provided Communication Systems

Policy: As with all assets, telephones, computers, email, mail and internet access are intended for authorized business use only.

Owner: Senior IT Manager

3.11.2 Electronic Message Usage

Policy: The electronic mail system is a company resource that provides business communication between users, students, vendors etc... Company communication systems and information resources are to be used for authorized business purposes. Personal use of email is discouraged. All email messages are company records and the company reserves the right to access and disclose the contents of any message sent over its electronic mail system. Users waive their right of privacy in electronic mail message and consent to access by the Company for any purpose. Users of the email system should be aware that all messages, sent or received are available for review by the company.

Commentary: This policy seeks to clarify who can read electronic mail messages, as well as the circumstances where messages can be examined. This policy puts associates on notice that their electronic mail may be monitored.

Owner: Senior IT Manager

3.11.3 Phone Usage

Policy: The phone system is a company resource that provides business communication between users, students, vendors and others. Company communication systems and information resources are to be used for authorized business purposes. Personal use of the phone system is discouraged. All phone conversations are company records and the company reserves the right to access and disclose the contents of any conversation taking place on its phone system. Users waive their right of privacy in phone calls and consent to access by the Company for any purpose. Users of the phone system should be aware that all conversations are available for review by the company.

Commentary: This policy seeks to clarify who can listen to phone conversations,, as well as the circumstances where conversations may be examined. This policy puts associates on notice that their phone conversations may be monitored.

Owner: Senior IT Manager

**3.12 Physical Security**

3.12.1 Office Access

 Policy: Each office is locked and requires a key card for access.

 Exceptions: Guests

 Owner: Senior IT Manager

3.12.2 Granting Employee Office Access

 Policy: Employees are granted key card access at the time they are hired.

Commentary: Only authorized members of the Technology Team can activate key cards.

Exceptions: Employees may have access to multiple locations.

 Owner: Senior IT Manager

3.12.3 Revoking Employee Office Access

Policy: Employee key card access is revoked after the employee’s last day.

Commentary: Only authorized members of the Technology Team can revoke key card access.

Owner: Senior IT Manager

3.12.4 Granting student access to the Phoenix Campus

Policy: Students enrolled in the BSN (Pre-Licensure) Program are granted key card access to campus on the first day of class.

Commentary: The Office Manager for the Phoenix campus submits a list of students that require access through ZenDesk.

 Owner: Senior IT Manager

 Effective Date: March 1, 2019

3.12.5 Revoking student access to the Phoenix Campus

Policy: Students access to campus is revoked when they are no longer attending the University.

Commentary: The Technology Team reviews student status once per month for students enrolled in the BSN (Pre-licensure) Program. Students who are no longer attending have their keycard access revoked.

Exceptions: The Office Manager, or a designated Aspen University employee can submit a request to the Technology Team to have an individual student’s key card access revoked at any time.

 Owner: Senior IT Manager

 Effective Date: March 1, 2019

3.12.6 Employee Key Card Sharing

 Policy: Employees must not share their key card with unauthorized persons.

 Owner: Senior IT Manager

3.12.7 Physical Access Control to Confidential Information

Policy: Access to every office or work area containing confidential information must be physically restricted to limit access to those with a need to access the confidential Information.

Owner: Registrar

3.12.8 Physical Access to IT Rooms are restricted to authorized personnel

Policy: IT Rooms are locked either with a physical lock or by key card access. Only authorized personnel have access to the IT Room.

Commentary: The VP of Systems or Senior IT manager determine authorization.

Exceptions: New York (new location).

Owner: Senior IT Manager

3.12.9 Physical Access to student records is limited to authorized personnel

Policy: The Registrar of each University is responsible for managing the student’s physical record. A student’s physical record is located in either a locked filing cabinet, office or workspace. Only employees authorized by the Registrar can access a student’s physical record.

 Owner: Registrar

**3.13 Application Security**

3.13.1 Change Control

Policy: All code changes affecting IT Production Servers must follow the Change Control & System Development Policies.

Commentary: See *Software Development* *Policy*.

Exceptions: Urgent issues that require immediate action are resolved immediately, but may be documented and reviewed afterwards.

 Owner: VP, Technology

3.13.2 Separation between Production and Development Servers

Policy: Application software in development is separate from production application software.

Commentary: Development and Production servers have their own environments.

Owner: VP, Technology

3.13.3 Actual student accounts are not used when testing.

Policy: The Technology Team creates and configures custom accounts for testing software that do not affect the actual student body of either University.

Exceptions:

Owner: VP, Technology

3.13.4 Deploying Code to Production Servers

Policy: Developers cannot deploy code to a Production Server.

Commentary: The only employees authorized to deploy code to a Production Server are the VP, Technology, VP, Systems and designated Technical Product Analysts.

Exceptions: Specific developers are granted access to Production Databases to resolve student and employee inquiries that are logged via ZenDesk.

Owner: VP, Technology

3.13.5 Code Review

Policy: Code reviews are required before software can be move into a production environment. Code reviews must be performed by an individual other than the originating author.

Exception: Urgent issues that require immediate action are resolved ASAP, but may be documented and reviewed afterwards.

Owner: VP, Technology

**3.14 Employee & Student Inquiries**

3.14.1 Technology requests are sent through ZenDesk

Policy: AGI’s Technology Team utilizes ZenDesk to track technology inquiries and requests.

Commentary: ZenDesk is a comprehensive Service Desk solution that AGI uses to manage technical inquiries.

Exceptions: In cases where someone contacts the technology team directly, the technology employee will determine if the communication should also be logged in ZenDesk.

Owner: VP, Systems

3.14.2 Dispositioning prospective and current student inquiries.

Policy: The CRM and Student Information System are able to log student inquiries and present them to employees for reporting purposes.

Commentary: The employee that interacts with a student can log that communication in the CRM or Student Information System.

Exceptions: The employee determines if the interaction requires tracking.

Owner: VP, Systems

3.14.3 Employee’s technical inquiries are logged via ZenDesk.

Policy: ZenDesk tracks employee inquiries, communication and status of each inquiry.

Commentary: ZenDesk allows AGI to track details related to the inquiry, and provides on-demand reporting to review trends.

Owner: VP, Systems

**3.15 Data Retention & Backups**

 3.15.1 Production Database Backup (In-House)

Policy: All production databases are backed up every 24 hours.

Owner: VP, Systems

3.15.2 Production Database Backup (In-House) Storage

Policy: Production database backups are securely stored with Amazon Web Services.

Commentary: AGI retains in-house backups on Amazon Web Services for 12-months.

Owner: VP, Systems

3.15.3 Production Database Backup (3rd Party)

Policy: Rackspace performs a full backup on all production databases every Friday, and incremental backups on other days.

Commentary: Rackspace retains backups for two-weeks.

Exceptions: Cloud DB Servers (USUGP, SQL04)

Owner: VP, Systems

3.15.4 Call Recording Retention (In-House)

Policy: Phone conversations taking place on AGI’s phone system are stored indefinitely.

Commentary: The Technology Team retrieves call recordings from the 3rd party and stores them in-house.

Owner: VP, Systems

3.15.5 Call Recording Retention (3rd Party)

Policy: Five9 retains call recordings for 60-days.

Owner: VP, Systems

3.15.6 Email Retention

Policy: The company utilizes Gmail for all corporate communication. Gmail retains email indefinitely. Email messages are accessible through Google Vault.

Exceptions: Emails that are deleted from the trash folder are not retained.

Owner: Senior IT Manager

3.15.7 Official Transcript Retention

Policy: Each University retains Official Transcripts received by students indefinitely. Transcripts are stored in electronic and physical format.

Commentary: Hard copies of Official Transcripts are securely stored on-site.

Owner: Registrar

3.15.8 Electronic Student File Retention

Policy: Each University retains a student’s electronic file indefinitely.

 Owner: Registrar

3.15.9 Workstation storage is cleared before being reissued.

Policy: Each workstation’s storage is completely cleaned before being reissued.

Commentary: The computer’s hard drive is completely wiped.

 Owner: Senior IT Manager

 3.15.10 Confirm backup restoration process works.

Policy: AGI maintains a Disaster Recovery Policy and tests backup restoration once per year.

Commentary: VP, Systems and VP, Technology perform the backup restoration test and document the process.

 Owner: VP, Systems

Approved By:

|  |  |  |
| --- | --- | --- |
| Name:  | Michael Mathews | Joseph Sevely  |
| Title:  | CEO | CFO |
| Signature:  |  |  |
| Date: |  |  |