integ

Table of Contents

Anderton Group II LTD Family of Integ Companies

Privacy Accreditations

(Find individual documents in this folder location)

SSAE16

Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, was finalized by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) in January 2010. SSAE 16 effectively replaces SAS 70 as the authoritative guidance for reporting on service organizations. SSAE 16 was formally issued in April 2010 and became effective on June 15, 2011.

SSAE 16 was drafted with the intention and purpose of updating the US service organization reporting standard so that it mirrors and complies with the new international service organization reporting standard – ISAE 3402. SSAE 16 also establishes a new Attestation Standard called AT 801 which contains guidance for performing the service auditor's examination.
Many service organizations that previously had a SAS 70 service auditor's examination ("SAS 70 audit") performed converted to the new standard in 2011 and now have a SSAE 16 report instead - also referred to as a Service Organization Controls (SOC) 1 report.

Additional information on SSAE 16 and Service Organization Control reports can be viewed at the AICPA's new web page (http://www.aicpa.org/soc).

Anderton Group II LTD has both **SOC1** and **SOC2** reports finalized December 16, 2016. These reports are available in this same folder.

We are **HIPPA certified**. HIPAA stands for the Health Insurance Portability and Accountability Act and is a U.S. federal law enacted in 1996 as an attempt at incremental healthcare reform.

We do have a **Privacy Policy** for PostalMethods.

Our **Employee Non-Disclosure** must be signed by all employees.

Cyber Risk Insurance Coverage for $1,000,000 Aggregate Limit – See Declaration page for details

Integ

Type II Service Organization Control Report (SSAE No. 16)

Independent Report on a Description of a Service Organization’s System and the Suitability of the Design and Operating Effectiveness of the Controls for the period of December 1, 2015 through November 30, 2016.

KirkpatrickPrice

Kirkpatrick Price, LLC
1228 East 7th Ave., Suite 200
Tampa, FL 33605

TABLE OF CONTENTS

KirkpatrickPrice
1228 East 7th Ave. Suite 200
Tampa, FL 33605

December 15, 2016

David Anderton, President and CEO
Integ
700 W. Loop 340
Waco, Texas 76710

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of the Controls

Scope
Throughout the period December 1, 2015 to November 30, 2016, we have examined Integ's description of its transactional printing system and examined the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Integ's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Integ uses Xerox subservice organization for high volume printer services. The description on pages 4 to 22 includes only the control objectives and related controls of Integ and excludes the control objectives and related controls of Xerox. Our examination did not extend to controls of the Xerox.

Service Organization's Responsibilities
On pages 4 and 5 of the description, Integ has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Integ is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the

related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period of December 1, 2015 to November 30, 2016.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described on pages 4 and 5. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in the organization's services. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in Integ's assertion on pages 4 and 5,

a) The description fairly presents the transactional printing system that was designed and implemented throughout the period December 1, 2015 to November 30, 2016.

b) The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period December 1, 2015 to November 30, 2016 and user entities applied the complementary user entity controls contemplated in the design of Integ's controls throughout the period December 1, 2015 to November 30, 2016.

c) The controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved and operated effectively throughout the period December 1, 2015 to November 30, 2016.

Description of Tests of Controls
The specified controls tested and the nature, timing, and results of those tests are listed on pages 23 to 66.

Restricted Use
This report, including the description of tests of controls and results thereof on pages 23 to 66, is intended solely for the information and use of Integ, user entities of Integ's transactional printing system during some or all of the period December 1, 2015 to November 30, 2016, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

CPA

Damon Sullivan, CPA
KirkpatrickPrice, LLC

Integ's Assertion

We have prepared the description of Integ's transactional printing system for user entities of the system during some or all of the period December 1, 2015 to November 30, 2016, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that:

1) The description fairly presents the transactional printing system made available to user entities of the system during some or all of the period December 1, 2015 to November 30, 2016 for transactional printing. The criteria we used in making this assertion were that the description:
    a) Presents how the system made available to user entities of the system was designed and implemented to process relevant transactions. These transactions include:
        i) The classes of transactions processed.
        ii) The procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities of the system.
        iii) The related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities of the system.
        iv) How the system captures and addresses significant events and conditions, other than transactions.
        v) The process used to prepare reports or other information provided to user entities of the system.
        vi) Specified control objectives and controls designed to achieve those objectives.
        vii) Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.
    b) Does not omit or distort information relevant to the scope of the transactional printing system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the systems and the independent auditors of those user entities, and may not, therefore, include every aspect of the transactional printing system that its auditor may consider important in its own particular environment.

2) The description includes relevant details of changes to the service organization's system during the period covered by the description.

3) The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period December 1, 2015 to November 30, 2016 to achieve those control objectives. The criteria we used in making this assertion were that:

a) The risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization.
b) The controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.
c) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

OVERVIEW OF SERVICES PROVIDED

The Anderton Group began in June of 1994 with the purchase of Brazos Printing. Over the next several years, sales doubled due to customer commitment and the quality of the company's products and services.

In 1996, the company took a new step with the acquisition of Cen-Plex Mailing, a 24-year veteran of the mailing business.

Next came Gatesville Printing, then Prim's Mailing Center. Through innovation and equipment enhancements, The Anderton Group became a leader in the full-service mailing industry.

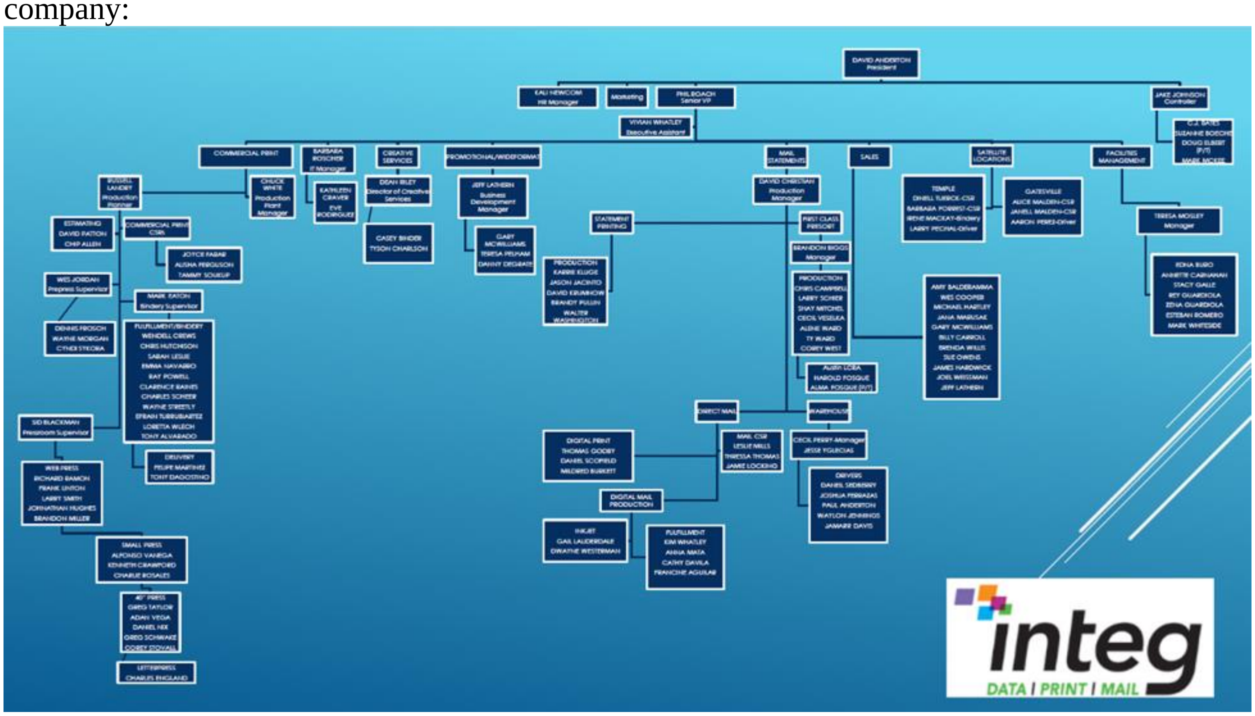
2001 brought the purchase of a manufacturing facility large enough to house the company's growing mailing operations. By this time, a name change was needed to represent the company's capabilities, and MailMax Direct began its life.

Additional acquisitions to Anderton Group over the past few yours included Direct Mail Partners in Tyler Texas, PMP Printing in Temple, Texas and the latest being Central Texas Printing in Waco, Texas. These acquisitions strengthened the services position within Anderton Group.

Now, Integ brings full integration of data, print, and mail capabilities, as well as traditional and digital marketing muscle, to the company's ever-growing client roster, while maintaining the highest integrity to both the clients and employee family.

Organization

An organization chart is maintained to highlight the division of responsibility within the company:



Management Control

Management's communication sets the tone and direction for the entire company. Security training is conducted on an annual basis. The organization maintains a principle called "Integ Way" that guides operational procedures. The Integ Way places focus on organization excellence and client experience.

The organization maintains a process for reviewing policies. The review process is completed by multiple managers and senior leadership and ultimately approved by the President/CEO. The policy is reviewed annually.

Monitoring activities are performed by management to ensure operational quality and control. An Integ Error report process is in place. When an error is made, the manager calculates how much the error costs in time and paper, then they sit down with the employee and go over the report and the cost. The files are kept and if the same employee continues to make errors, then write ups are conducted.

Management staff routinely perform a review of the status of each processing workstation system. The review process looks for the condition of each customer account folder, data files, or other abnormalities. Management staff performs random auditing of customer data processing by Integ operators. Random audits occur physically next to the operator as the operation performs tasks. These audits look for errors in processing, deviations from standard procedures, and other abnormalities in processing.

Management staff perform code review and process review on the components of each customer application submitted to be placed in live production state. In order for a customer application to be placed in live production state, the customer application must be approved by these review processes. These reviews look for accuracy of customer data, security of the customer data, abnormalities which could potentially cause errors or accidental or purposeful exposures of or changes to data.

In the event that any of these control methods raises an issue, an attempt is made to correct the issue. If possible, supervisors offer more training and reprimand the operator is necessary.

Integrity and Ethics

The organization maintains an employee handbook that is printed and shared with new hires and all employees annually. The handbook is distributed sooner if there is a change and re-acknowledgement is required. The handbook covers:

- Code of Conduct
- Ethics
- Reference Checks
- Discipline

Controls Related to Personnel

Job Descriptions

Job descriptions are maintained for critical positions within the company. Job descriptions document the following information:

- Position Title
- Department
- Reports To
- Salary Range
- Position Summary
- Essential Job Functions
- Essential Job Requirements
    - Education
    - Experience
    - Required Skills
    - Preferred Skills
    - Physical Requirements

Hiring, Termination, and Personnel Changes

Hiring and termination policies and procedures are maintained to guide the onboarding and offboarding processes. Once a job offer has been accepted, a criminal background screen is processed. Upon a clear criminal background screen, a drug test is ordered. Upon negative drug test results, new hire paperwork and training begins. A new hire checklist is followed.

The formal new hire packets include all relevant materials, company disclosures, and documented expectations of management. A termination checklist is followed for all terminations.

Training

All employees are trained on sexual harassment (via video), security (via powerpoint) and GHS (via a written document). Following the sexual harassment and GHS training, quizzes are given.

RISK ASSESSMENT

Integ management performed risk assessment during the design and implementation of the control objectives and related controls described in this report. As part of its risk assessment, management identified the threats and vulnerabilities relevant to the security of Integ business operations and rated the risk posed by each identified vulnerability. This rating allowed for the design and implementation of controls to mitigate the most significant risks to the security of Integ's service.

Risk assessment is performed by Integ semi-annually and in response to any update to the design and implementation of the control objectives and related controls described in this report.

When conducting risk assessment, Integ first identifies threats and vulnerabilities relevant to the security of its business operations. Integ then – for each identified vulnerability – considers:

a) The likelihood of impact (i.e., the likelihood of the vulnerability being exploited), and

b) The severity of impact (i.e., how damaging an exploitation of the vulnerability would be).

These estimations of impact potential and impact severity are then used in conjunction to establish a risk ranking for each vulnerability. If a vulnerability is unlikely to be exploited and would have a minor impact, it is viewed as a relatively small risk. If a vulnerability is very likely to be exploited and would have a severe impact, it is viewed as a very significant risk. Other combinations of likelihood and severity (high likelihood, low impact; low likelihood, high impact; moderate likelihood, moderate impact; etc.) result in establishment of a risk ranking somewhere along this continuum.

Once the severity of risk posed by each identified vulnerability has been broadly quantified, Integ management ensures that the design and operation of its controls are sufficient to address all significant risks to the security of its operations.

The following types of risk are identified in Integ's risk assessment process:

- Operational risks associated with information systems, manual processes, and external systems
- Financial and legal risks associated with market and organizational changes, regulatory costs, or other negligent action
- Technology risks associated with intrusion, system failure, and errors

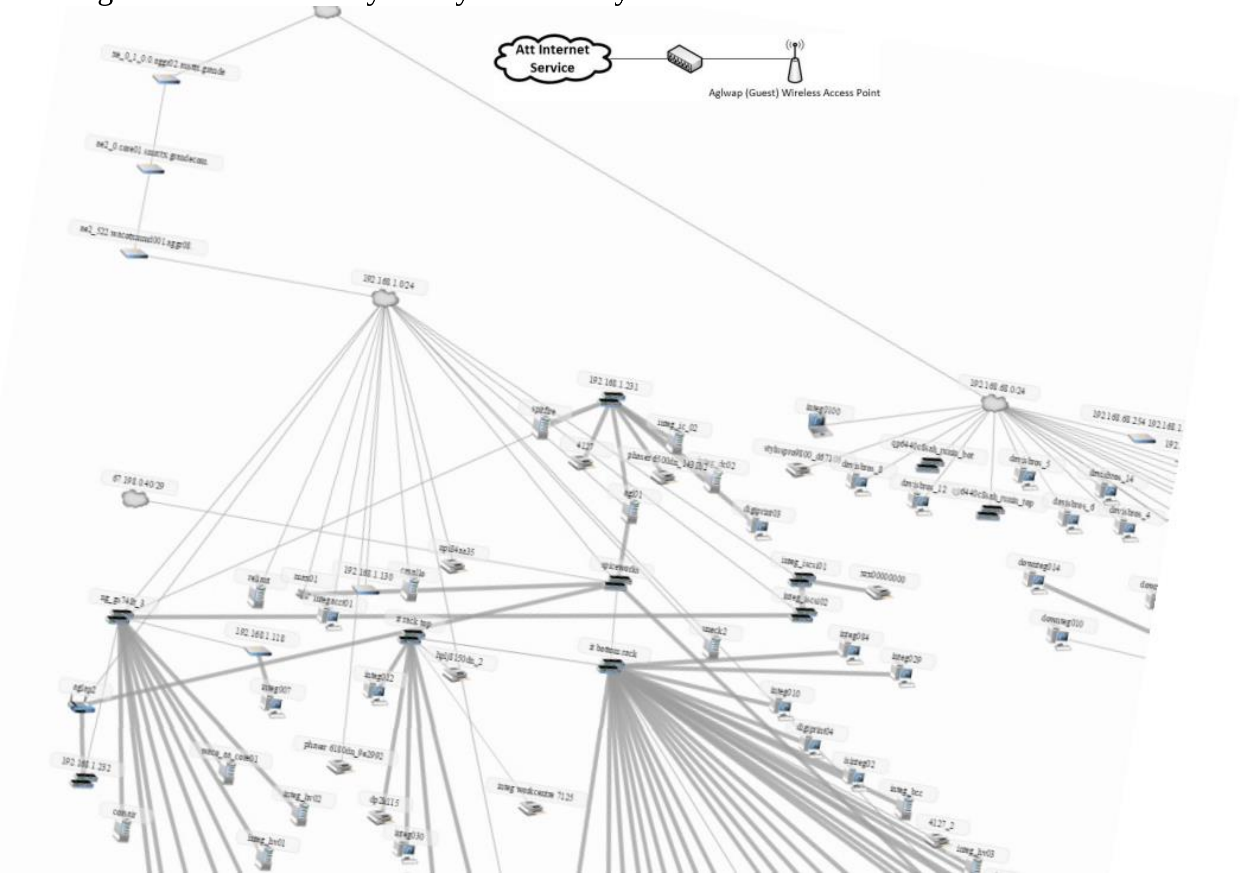
MONITORING

The management and supervisory personnel of Integ monitor performance quality and control operation as a normal part of their activities. The organization has implemented a series of “key indicator” management reports that measure the results of various processes involved in providing transaction processing to customers. Key indicator reports include reports that identify various computerized information system events, such as failed access attempts, rejected items, deviations from scheduled processing, and program changes.

These reports are periodically reviewed (depending on the nature of the item being reported on) by appropriate levels of management, and action is taken as necessary. Depending on the nature, age, and amount (as applicable) of processing exceptions, they are referred to higher levels of management for review.

Description of Computerized Information Systems

A network diagram is maintained to highlight the interconnectivity of the network environment. The diagram is maintained by the Systems Analyst:



General IT Controls

Information Security Program

The organization maintains an information security policy to govern the operating environment. The policy is reviewed at least once annually and covers legal, regulatory, and industry standards. Responsibilities for information security is reinforced in an annual security awareness training program.

The organization distributes the information security policy to personnel and business partners. Each policy administrator has a pdf copy of the policy that can be printed or emailed as requested by existing employees or business partners. A paper copy is distributed in the new employee packet as well as signed off and given to employees yearly. An NDA is signed any external party before sharing any sensitive information.

The organization maintains a process whereby users are provided a process for informing the organization about security breaches and for submitting complaints. In the event that a customer, data owner, IT personnel, or Information Technology Services representative identifies a potential security incident involving a computer, the computer must first be disconnected from the network, then shutdown. In all instances, the Operating Unit awaits further instructions prior to continued operation of the computer.

Any employee or data owner who believes that a security incident has occurred must immediately notify their supervisor, HR, or any IT personnel. There is also a suggestion box outside of the HR Office that can be used in situations where the person reporting wants to remain anonymous. Upon notification by an employee, IT personnel promptly handle the incident according to the incident response and procedure policy.

In the event of loss or theft of customer materials or mailpieces, the customer owning those items is also notified by contacting either the primary customer lead contact or contacts specified in any contract or contact list with the customer. Internal complaints can be made directly to a supervisor, HR, IT department or in the suggestion box located outside of the HR office.

Incident Response

The organization maintains incident response policies and procedures. The following steps are taken:

1. Incident Identification
2. Reporting and Incident Declaration Procedures
3. Incident Severity Classification
    a. Level 1 - One case of potentially harmful activity
    b. Level 2 - One definite example of harmful activity or multiple examples of potentially harmful activity
    c. Level 3 - Major attempted or successful security breach or multiple examples of harmful activity
4. Typical Response Procedures
5. Root Cause Analysis and Lessons Learned
6. Plan Testing and Training
7. Critical Systems Restore Strategy

Environmental Security

The organization has implemented environmental controls. The computer room is located within the IT office and has biometric locks on the front and rear entrance along with a separate HVAC system with the temperature set to 65. IT Watchdog temperature and humidity sensors are in place and provide email alerts.

The computer room is located on the first floor of a one-story facility and does not have raised floors. The entire facility has fire and smoke alarms with wet pipe fire extinguishers, including the computer room and smoke and heat detectors tied to the same system.

Physical Security

Physical security controls are in place to protect secure areas. After hours, employees must have a key code to get into the facility as well as a code to turn off the alarm system. Alarm codes and key codes are immediately changed when personnel are terminated. Any visitors must sign in before entering the facility. All visitors must be accompanied by an AGL employee. Biometric locks are used for the IT department. Locked containers are used for PHI information that will be shredded at a later date.

Doors are locked Monday-Friday at 5 PM. During this time, individuals must use the door code to gain access. The security alarm is set by the last person leaving for the night and disarmed by the first person in the morning. The CEO receives a monthly report from the alarm company with all activity.

Security cameras cover each of the entrances into the building. The organization also maintains cameras that display areas within the facility that might contain sensitive information. Ten cameras are maintained and the DVR retains camera footage for at least 90 days.

The organization maintains a visitor log. Visitors are required to sign the visitor log at the reception desk. The logs contain the following information:

- Visitor name
- Data
- Time in
- Time out
- Reason/business name
- Escorted by

Logical Access

The organization maintains a policy on access rights and privileges granted to user IDs. User IDs are based on the user's first initial and last name. A new employee IT form is filled out and signed by HR, Supervisor, and IT. Privileges are assigned according on a need-to-know basis according to job function. Active Directory is used as the organization’s automated access control system. Two-factor authentication is used for secure login.

Access to server partitions is only granted to authorized AGL employees using approved internal software on approved workstations on the AGL premises. Access is controlled by authorized AGL IT administrators. Short term access of at-risk data such as workstation client access operations is limited to each in-use session by an authorized AGL employee on a workstation approved for such access by AGL IT administrators within the AGL premises.

In the event of termination of an employee, HR notifies IT immediately so that the user can be withdrawn from any privileges on the network. The user password and email passwords are changed immediately. For some employees, the account is deleted immediately. For others, files are removed from their accounts as needed, and emails are forwarded for 30 days. After 30 days, their account is re-evaluated. At that time, the account is removed if it is no longer in use.

AGL employee user accounts and passwords are controlled by authorized AGL administrators. Passwords must be changed every six months. User accounts and passwords control access to network partitions, workstations, servers, and other services and applications.

The organization maintains a process for registering/de-registering users for online access to services. On the SFTP site, the company has one username/password to upload files. This is mainly due to them having automated the process and it is a server connecting and uploading a rather than an individual.

Network Monitoring

The organization maintains network monitoring/logging processes. SpiceWorks actively scans network devices, including workstations, servers, printers, etc. It provides and manages alerts on the following items:

- Equipment
- HelpDesk Tickets issued by employees
- A timeline of tickets and other network events
- Details on Antivirus (Sophos) versions, installations, and updates
- An inventory summary with equipment details
- Software patches with priority

This information and reports are accessed by IT Personnel only. Reporting data cannot be modified.

The organization maintains a process to monitor system capacity and plan for future requirements. Integ performs a monthly analysis on its servers. When the company notices that it is below 10% free space on servers, IT takes steps to see if more space can be allocated. If not, then Integ makes plans to add more drives or replace equipment. Integ also receives notices from SpiceWorks if a volume goes below 10% free space.

Monitoring is performed to limit information leakage. SpiceWorks provides a scan of the network so Integ can view inventory of all hardware, software, applications, and equipment connected to the network. SpiceWorks also detects unwanted devices on the network that may be stealing bandwidth or confidential company information. Regular scans allow Integ to eliminate internal equipment theft and also detect malfunctions before they deal permanent damage.

Sophos provides intrusion detection as well as visual alerts to the users and email alerts to IT staff. The firewall also prevents intrusions by restricting both inbound and outbound traffic according to the rules set up. Locked containers are provided to dispose of confidential customer information. Computers require passwords to prevent anyone obtaining confidential information. IT area has biometric locks to prevent unwanted access to servers and workstations that have administrative rights.

Configuration Management

A change management process is in place. The process captures:

- CR #
- Department
- Date
- Location
- Phone
- Description
- Changed needed by date
- Reason for change
- Request sign off
- Approver
- Change type
- Change priority
- Environments impacted
- Resources required
- Test plan description
- Rollback description
- Implementation test results

The organization maintains a process for testing and approving network changes. A change request form is filled out and approved. In systems where there is not a test environment, the config is saved prior to the change so that if a problem is detected, it can immediately be put back to the original configuration.

Systems are configured with the latest patches and software updates along with antivirus protection. Group Policy is configured for complex passwords. SpiceWorks monitors and scans the network daily for any changes or additions to the network. An email alert is sent the IT department when there have been additions so they may be verified. Any systems added to the network must go through the change management process and will be verified that it meets Integ criteria. Integ has established a workstation and server install checklist to make sure the criteria are met.

Servers are subject to standard security management practices which include keeping them up-to-date by applying the approved patch management processes. Antivirus is installed on all devices, which includes network intrusion detection, on-access scanning, and antivirus and tamper protection. The ability to install or remove software is limited to users with administrative privileges. Software versions are kept up to date through the change management network changes. Network topology documentation is maintained.

Hardening standards are based on NIST SP 800-53. The main department is responsible for information security along with defining the infrastructure. Integ has implemented firewalls and security and monitoring standards that permit or deny users access to the system. Patches are applied as necessary. Service accounts that are not used are removed or disabled. Unnecessary software is removed from servers and workstations.

Personnel with responsibilities for system configuration stay knowledgeable of appropriate ways to securely configure the organization's systems:

- Security technology websites such as TechWorld, NetworkWorld, and SecurityWeek are used.
- Personnel follow Sophos presentations and updates on new threats.
- The SpiceWorks Community is monitored for latest in network monitoring and threats.
- Personnel read appropriate security bulletins available from vendors, user groups, and security institutes.
- Personnel ensure that servers are secured physically where no unauthorized person can access them.

Changes that may affect system availability and system security are communicated to management and users who may be affected. When changes need to be made, a short description of changes scheduled for implementation is sent by email. This email is distributed to all Integ employees (including management), change representatives of affiliates, and key business partners.

Firewalls and routers are configured to limit traffic to that which is necessary for business purposes. The restrictions are defined on the SonicWALL as follows:

- Content Filter - Internet Content Filtering equips the SonicWALL to monitor usage and control access to objectionable web content according to established Acceptable Use Policies.
- Intrusion Prevention - Intrusion Prevention integrates a high-performance Deep Packet Inspection architecture and dynamically updated signature database to deliver complete network protection from application exploits, worms, and malicious traffic. In addition, Intrusion Prevention provides access control for Instant Messenger (IM) and Peer-to-Peer (P2P) applications.
- Gateway Anti-Virus - Gateway Anti-Virus integrates a high performance Real-Time Virus Scanning Engine and dynamically updated signature database to deliver continuous protection from malicious virus threats at the gateway.
- Anti-Spyware - Anti-Spyware prevents malicious spyware from infecting networks by blocking spyware installation at the gateway and disrupts background communications from existing spyware programs that transmit confidential data.
- RBL Filter - Real-time Black List

Vulnerability Management

Sophos Enterprise Console is used to automatically update devices. SpiceWorks informs Integ of any workstations that have out of date antivirus. The GPO checks and downloads vendor updates every day at 3 AM and then prompts users to install and reboot if required for the Windows OS. Server updates are pushed monthly. SpiceWorks checks warranty and patch notifications and is set to email alerts to IT for identified discrepancies.

Data Security

Integ receives sensitive data that includes bank statement info such as bank account numbers and amounts, insurance policy information, and information for utility bills. This data is stored, transmitted, and processed in a variety of formats, including PDF, PCL, .txt, .csv, .xls.

At-risk data within the AGL organization is only stored on secure servers or approved data medium(s) within approved areas in the AGL facilities. At-risk data stored in secured servers resides in password protected partitions with only authorized AGL employee access, on a restricted internal network. In the case of customer at-risk data, the data only remains stored for the duration of the processing of that data or for the required amount of time by the USPS or other authoritative bodies. Customer at-risk data must be removed as soon as allowable. At-risk data is not stored on workstations for any time longer than in-session required accessing or processing. At-risk data is not stored on portable computers at any time. Data files from customers are deleted from the system within one week of receipt.

If PHI documents are uploaded to Integ's servers, Integ asks the customer to give them a count of the uploaded documents. Integ then verifies the number of documents processed against the customer's number. If there are any discrepancies, the documents are held until the matter is resolved.

Backup and Restoration

The organization maintains backup policies and procedures. The following controls are in place for backup procedures:

- IT staff are responsible for ensuring that backup copies of all confidential information on Integ electronic media and information systems are made regularly. This includes both confidential information received by Integ and created within Integ. Information systems and electronic media include file servers, database servers, and Domain Controllers and web servers.
- IT staff are responsible for ensuring that Integ has adequate backup systems that ensure the ability to create and recover data following a disaster or intentional destruction of data or equipment failure. Specific data must be stored at a remote location that is a sufficient distance from Integ facilities to escape damage from a disaster at Integ.
- IT staff are responsible for ensuring that backup copies of information stored at secure remote locations are accessible to authorized Integ employees for timely retrieval of the information.
- IT staff are responsible for ensuring that backup media containing information at the remote backup storage site is given an appropriate level of physical and environmental protection consistent with the standards applied to information physically at Integ.
- Backup and restoration procedures for Integ electronic media and information systems containing information must be regularly tested by IT staff or designee to ensure that they are effective and that they can be completed within a reasonable amount of time.
- The retention period for backup of information on Integ information systems and any requirements for archive copies to be permanently retained must be defined and documented by the Information Security Officer.

Business Continuity and Disaster Recovery

The organization maintains a business continuity/disaster recovery plan that covers the following items:

- Scope of Disaster Recovery Plan
    - List of Operations Covered
    - Operation Detail
- Risk Assessments
    - Natural Disaster/Emergency Definitions
    - Technical Disaster/Emergency Definitions
    - Human Emergency/Threat Definitions
    - Failure Scenario Impact Analysis
- Operational Priorities
    - Critical Operations
    - Critical Operational Personnel
    - Critical Equipment
    - Critical Applications
    - Critical Data
    - Critical Documents / Materials
- Redundant Off-Site Locations
    - Off-Site Locations
    - Redundant Operations
    - Redundant Equipment
    - Third-Party Equipment Support
- Disaster Recovery Procedures
    - Safety Issues
    - Disaster Recovery Triggers
    - Disaster Notification
    - Disaster Recovery Activation
    - Damage Assessment
    - Equipment Protection and Salvage
    - Emergency Procurement Procedure
    - Off-Site Preparations
    - Operational Priority Review
    - Individual Service Continuity Procedures
    - Processing Cycle and Reporting
    - Returning to Normal Operations

SUBSERVICE ORGANIZATIONS

Integ uses industry-recognized subservice organizations to achieve operating efficiency and to obtain specific expertise. Integ periodically reviews the quality of the subservice organizations' performance.

The following are the principal subservice organizations used by Integ:

- Xerox - services and support to High Volume Printers.
- Grande Communications - ISP and phone provider
- Dell - Server/firewall warranty and support
- Encore/TXU - Electricity provider

USER CONTROL CONSIDERATIONS

Integ's services are designed with the assumption that certain controls will be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report. Integ's management makes control recommendations to user organizations and provides the means to implement these controls in many instances. Integ also provides best practice guidance to clients regarding control element outside the sphere of Integ responsibility.

This section describes additional controls that should be in operation at user organizations to complement the Integ controls. User control recommendations include:

- User organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with Integ.

- User organizations should ensure timely removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with Integ's services.

- Transactions for user organizations relating to Integ's services should be appropriately authorized, secure, timely, and complete.

- For user organizations sending data to Integ, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.

- User organizations should implement controls requiring additional approval procedures for critical transactions relating to Integ's services.

- User organizations should report to Integ in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Integ.

- User organizations are responsible for notifying Integ in a timely manner of any changes to personnel directly involved with services performed by Integ. These personnel may be involved in financial, technical or ancillary administrative functions directly associated with services provided by Integ.

- User organizations are responsible for adhering to the terms and conditions stated within their contracts with Integ.

- User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by Integ.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Therefore, each client’s system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

SECTION III:
INFORMATION PROVIDED BY THE INDEPENDENT SERVICE AUDITOR

Section III outlines the controls in place by Integ and describes the tests of their effectiveness performed by the independent service auditor. The following methodologies were used in testing the suitability of the design and operating effectiveness of Integ's controls:

Test Methodology	Description
Interview	The auditor inquired of relevant personnel to corroborate control placement or activity.
Review	The auditor obtained and read relevant Integ documentation.
Observation	The auditor directly witnessed control placement or activity or evidence thereof.

The tables on the following pages outline the control objectives, controls in place, and independent testing relevant to the independent assessment of Integ's control environment throughout the period December 1, 2015 to November 30, 2016.

Control Objective 1 - Organization and Administration

Control Objective 1: Controls provide reasonable assurance that management provides oversight and segregation of duties as well as guides consistent implementation of security practices.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results

1.1	Monitoring activities—including the use of an error documentation report—are used to ensure operational quality and control.	Reviewed Integ Error Documentation and selected a few samples from employee files which can rise to the level of disciplinary actions. When an error is made, the manager calculates how much the error costs in time and paper, then they sit down with the employee and go over the report and the cost. The files are kept and if the same employee continues to make errors, then write ups are conducted. These reports are also shared with Accounting to track loss and overages and account for them accordingly. Interviewed HR Manager to verify the following: • Management staff routinely perform a review of the status of each processing workstation system. The review process examines the condition of each customer account folder, data files, or other abnormalities. • Management staff performs random auditing of customer data processing by Integ operators. Random audits occur physically next to the operator as the operator performs their tasks. These audits look for errors in processing, deviations from standard procedures, and other abnormalities in processing. • Management staff performs code review and process review on the components of each customer application submitted to be placed in live production state. In order for a customer application to be placed in live production state, the customer application must be approved by these review processes. These reviews look for accuracy of customer data, security of the customer data, abnormalities which could potentially cause errors and accidental or	No Relevant Exceptions Noted

		purposeful exposures of or changes to data. • In the event any of these control methods raises an issue, an attempt is made to correct the issue. If possible, supervisors offer more training and reprimand the operator is necessary. Reviewed the Integ Error Report which includes only customer facing: • Date • Customer • Employee • Job name • Job Number • Material Cost • Labor Cost • Postage Cost • Customer Reaction • Remediation steps Observed that there are monthly management meetings and observed the minutes of the meetings for the past four month where QA and corporate goals and financial goals are discussed. Observed that "The Integ Way" is a new key initiative that provides financial oversight and sets operational goals. It is expected that managers will filter this down to their teams. Observed the job tickets using record counts to make sure all processing occurs as appropriate. The operations manager said that if counts are off that the job processing is stopped until the error is found.	

1.2	The organization maintains a network diagram to highlight the interconnectivity of the network environment.	Reviewed SpiceWorks Network Map. Interviewed Systems Analyst, who is responsible for the network diagram's maintenance and updates the documents any time there are changes made to the network. Observed the use of SpiceWorks inventory onsite and noted that this is autogenerated. Observed that SpiceWorks also maintains the system inventory. Onsite observation appears to corroborate what Spice Works is showing. The organization runs on a flat network. Observed and reviewed the firewall rules with LIVE-IT (outsourced network consulting company) and observed the rules that filter traffic on the public facing systems as needed.	No Relevant Exceptions Noted
1.3	The organization maintains a complete inventory of systems including virtual technologies.	Reviewed Server Rack Diagram and Virtual Servers spreadsheet and compared it to the physical and virtual server and noted that the inventory includes the server name, OS, and purpose. Observed there is one function per server and observed the SpiceWorks autogenerated reports onsite. This is overseen by the Systems Analyst. SpiceWorks captures the system name, function, whether physical or virtual and its identification information, CPU, memory, and disk load in real time. Both network diagram and inventory are maintained by SpiceWorks but a spot check of various systems onsite all showed up in SpiceWorks so the assessor has reasonable assurance that the organization is doing a thorough of this control.	No Relevant Exceptions Noted

1.4	The organization maintains marketing, contractual, or other materials that would describe the services or scope of works provided to clients.	Reviewed Integ Service Brochure. Reviewed Integ Website. Observed that the organization provides print, mail, data, marketing, and transactional services to clients. Interviewed HR Manager and Controller.	No Relevant Exceptions Noted
1.5	The company maintains a clearly defined organizational structure. An organization chart is in place to highlight the division of responsibility.	Interviewed HR Manager to verify that David Anderton is the company President. Three managers report directly to him: • Kali Newcom • Jake Johnson • Phil Roach Observed that Phil Roach has six managers who report directly to him as well as two satellite locations. Observed an appropriate segregation of duties and oversight for security. Reviewed Org Chart.	No Relevant Exceptions Noted

1.6	Management's communication sets the tone and direction for the entire organization.	Reviewed the following documents: • Integ Way document • Employee Handbook • Security Exam • Do's and Don'ts Handbook • Do's and Don'ts Password Guideline • Integ Way Committee Meeting Minutes Reviewed the onboarding and one ongoing training where they define Organization Excellence (OE) as ongoing improvement, promoting continuous flow of value to the client. OE is a mindset and applies to all areas. Reviewed security training and quiz as well as the Integ Way committee minutes to verify that training is being done at least annually. Observed that Integ performs security training on an annual basis. They currently have an Integ Way focus group to help implement that culture into the company. Observed the employee handbook has a - Standards of Conduct (section 5). Observed 3 of 28 new hires during the audit to verify they completed their new hire training.	No Relevant Exceptions Noted
1.7	The organization maintains a process for creating, approving, and maintaining the organization's policies.	Interviewed HR Manager to verify that the review process is completed by multiple managers and senior leadership and ultimately approved by David Anderton. The policy is reviewed annually. Observed from the majority of policies reviewed so far that all appear to have been reviewed or updated within the past year. This was corroborated with interview of the company owner David Anderson.	No Relevant Exceptions Noted

<table>
<tr><td>1.8</td><td>Management communicates and oversees the implementation of the Code of Conduct, Integrity, and Ethics to new and current employees.</td><td>Interviewed HR Manager.
Reviewed Employee Handbook to verify that section 5, chapter 11 of the handbook discusses conflict of interest and business ethics. Each employee signs a handbook acknowledgment.
Reviewed Internet and Email Policy to verify that monthly management meetings are held and managers are expected to filter down information to their teams.
Observes a sample of 3 of 28 new hires to verify that their signed acknowledgements were in place.</td><td>No Relevant Exceptions Noted</td></tr>
<tr><td colspan="4"><b>Control Objective 1 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that management provides oversight and segregation of duties as well as guides consistent implementation of security practices.</b></td></tr>
</table>

Control Objective 2 - Information Security Program

Control Objective 2: Controls provide reasonable assurance that information security policies are maintained, which set the security tone for the company and create security awareness.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
2.1	The organization has implemented privacy policies for handling personal information in accordance with relevant legislation and regulations.	Observed that there is a signed Proprietary Information and Non-Disclosure Agreement acknowledgement as part of the new hire process. Observed a sample of 3 of 28 new hires to verify that their signed acknowledgements were in place and retained in their employee files. Reviewed the Integ website and noted that confidential information is collected on the Contact Us form. Reviewed Proprietary Information document. Interviewed HR Manager.	No Relevant Exceptions Noted
2.2	The organization maintains an annual risk assessment process.	Interviewed IT Manager and Systems Analyst to verify that Integ reviews risks annually in line with NIST 800-14 and 800-18 guidance as they plan for their annual DR exercises. Observed that the risk assessment is based on hybrid model most closely aligned to NIST 800-30. *Exception*: There was no formal risk assessment conducted until 1/19/17 and so there was not sufficient time in place to assess its effectiveness.	Exception Noted

2.3	The organization maintains an information security policy to guide security practices.	Reviewed Information Security Policy to verify a revision history that shows the policy is reviewed at least once per year and also shows a description of changes. The policy covers legal, regulatory, and industry standards. Observed 3 of 28 new hires in the audit period to verify that their signed acknowledgment was in place and retained in their employee file. Interviewed IT Manager to verify that an annual review is performed in April.	No Relevant Exceptions Noted
2.4	The organization's security policies define information security responsibilities for all personnel.	Reviewed Security Exam. Reviewed Security Training presentation to verify that information security responsibilities are enforced. Observed the following security administrators: • David Christian • Kathy Craver • Barbara Roscher • Eve Rodriguez Observed reviews and updates are made and published annually or more frequently if needed. The latest revision is available from a policy administrator, accounting, or human resources. Security responsibilities belong to all employees of the company. This policy is part of the new employee training. Interviewed IT Manager.	No Relevant Exceptions Noted
2.5	The organization monitors third-party service providers' service delivery and compliance status.	Interviewed IT Manager to verify that service providers are monitored while services are performed. They do not have access to any confidential information. An IT employee works along with them any time they are in the system. Observed that onsite destruction is monitored by an Integ employee.	No Relevant Exceptions Noted

2.6	The organization maintains incident response policies and procedures.	Reviewed Incident Bank Incident document. Reviewed Incident Response Plan and Procedures. Interviewed IT Manager. Observed email chain of incident reports and lessons learned and corrective actions defined with the client, Independent Bank. Transactional customers contact their CSR or the manager of that department with any issues or concerns. In the case of a potential error on Integ's part, the manager contacts Integ's production manager for further investigation. The Production Manager checks reports from the production equipment, and if needed, contacts the Technology team. They produce relevant reports and evidence for the proposed error. Once the error has been discovered and researched, management responds to the customer with additional information and a proposed solution.	No Relevant Exceptions Noted
2.7	The information security policy is distributed to personnel and business partners.	Interviewed IT Manager to verify that each policy administrator has a pdf copy of the policy that can be printed or emailed as requested by existing employees or business partners. A paper copy is distributed in the new employee packet as well as signed off and given to employees yearly. Reviewed a sample of new hires to verify they have acknowledged the ISP. Observed that this is given to new hires and then annually thereafter and must be re-acknowledged. Observed a sample of 3 of 28 new hires to verify that their signed acknowledgment is retained in their file.	No Relevant Exceptions Noted

2.8	Training is given to personnel with security breach responsibilities.	Reviewed the following documents: • Proprietary Information document • Customer List – Data File Usage NDA • Security Training Acknowledgement • Security Policy Interviewed HR Manager. Observed that the Information Security Policy and NDAs must be acknowledged by new employees. Observed sample of acknowledgements listed in the HR section.	No Relevant Exceptions Noted

2.9	The organization ensures that clients and/or users are provided a process for informing the organization about security breaches and for submitting complaints.	Reviewed Information Security Policy to verify: • In the event that a customer, data owner, IT personnel, or Information Technology Services representative identifies a potential security incident involving a computer, the computer shall first be disconnected from the network, then shutdown. In all instances, the Operating Unit will await further instructions prior to continued operation of the computer. • Any employee or data owner who believes that a security incident has occurred, shall immediately notify their supervisor, HR, or any IT personnel. There is also a suggestion box outside of the HR Office that can be used in situations where the person reporting wants to remain anonymous. • Upon notification by an employee, IT personnel shall promptly handle the incident according to the Incident Response and Procedure policy. • In the event of loss or theft of customer materials or mailpieces, the customer owning those items also is to be also notified by contacting either the primary customer lead contact or contacts specified in any contract or contact list with the customer. • Internal complaints can be made directly to a supervisor, HR, IT department or in the suggestion box located outside of the HR office. Observed an email where a client reported an incident this year. It was followed up on, the cause was determined, and corrective action was	No Relevant Exceptions Noted

		taken to prevent the issue from occurring again and notification of these actions sent to the client.	
2.10	The organization protects system documentation against unauthorized access.	Interviewed IT Manager to verify that system documentation is kept on a network drive and backed up daily. Active Directory prevents anyone other than the appropriate staff to access this server/drive.	No Relevant Exceptions Noted
2.11	The organization maintains a non-disclosure agreement signed by third parties prior to sharing information with them.	Reviewed NDA, which is formally executed and signed with any external party before sharing any sensitive information. Interviewed IT Manager.	No Relevant Exceptions Noted
2.12	The organization ensures that the information security policy is reviewed and updated.	Reviewed Information Security Policy to verify the revision history. Interviewed IT Manager to verify that an annual review is performed in April.	No Relevant Exceptions Noted
2.13	Daily operational procedures—including daily log reviews—are performed to ensure the integrity of security processes.	Reviewed Daily Security Procedures that check for any errors or warnings that could be potential security issues. Any unusual findings are investigated immediately and reported to all IT personnel. Observed an example of the daily log review by the Systems Analyst that is sent to the Technology Department which includes the IT Manager for management review. Interviewed IT Manager.	No Relevant Exceptions Noted
Control Objective 2 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that information security policies are maintained, which set the security tone for the company and create security awareness.			

Control Objective 3 - Human Resources

Control Objective 3: Controls provide reasonable assurance that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. Controls ensure the reduction in risk of theft, fraud, and misuse of facilities.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
3.1	The organization maintains an employee handbook that communicates essential HR information.	Reviewed Handbook to verify that it covers: • Code of Conduct • Ethics • Reference Checks • Discipline Interviewed HR Manager. Observed a sample of 3 of 28 new hires during the audit period to verify they signed the Employee Handbook acknowledgement and NDA & Confidentiality acknowledgements and that their background checks were conducted by PublicData.com. Observed that the handbook is printed and shared upon new hire and annually thereafter, or sooner if there is a change and re-acknowledgement is required.	No Relevant Exceptions Noted

3.2	Job descriptions are maintained for all critical functions in the organization.	Reviewed the following job descriptions: • Drivers • Presort Manager • Production Manager • Client Service Representative • Baylor Site Manager • Controller • Human Resources Manager • Pressroom Supervisor • Operations Manager • Sales and Client Service Manager • IT Manager • Warehouse Supervisor • Creative Services Director • Wide Format Production Observed that job descriptions are formally documented for all critical function in the organization.	No Relevant Exceptions Noted
3.3	Hiring and termination policies and procedures—including appropriate documentation—are in place for both	Reviewed New Employee Checklist and Employee Termination Checklist to verify that the process is formally documented to capture all the necessary steps for setting up access and then removing and revoking as appropriate. Once a job offer has been accepted, a criminal background screen is processed. Upon a clear criminal background screen, a drug test is ordered. Upon negative drug test results, new hire paperwork and training begins. A new hire checklist is followed. Interviewed HR Manager. Observed the formal new hire packets includes all relevant materials, company disclosures, and documented expectations of management.	No Relevant Exceptions Noted

3.4	The organization maintains a process for conducting background checks using PublicData.	Interviewed HR Manager to verify that background checks are conducted on all employees (FT, PT, and Temp) prior to working for the company. PublicData is used for employees hired by the company. Employees hired through the temporary agency are screened through the temporary agencies companies. Observed a sample of 3 of 28 new hires during the audit period. Due to the nature of the work, the organization does not perform educational, reference checks, or employment verification. Observed the following components were covered under the background checks: • Criminal • SSN • Name verification • Photo ID • Drug screen • NDA	No Relevant Exceptions Noted
3.5	Training programs have been implemented by the organization.	Interviewed HR Manager to verify that all employees are trained on sexual harassment (via video), security (via powerpoint) and GHS (via a written document). Following the sexual harassment and GHS training, quizzes are given. This is conducted at new hire. Sexual harassment training happens annually and there is a quiz that goes into their file. Observed 3 of 28 new hires in the audit period and observed their signed acknowledgments for: • Sexual Harassment Training • Information Security Policy • Information Security Awareness Training	No Relevant Exceptions Noted
Control Objective 3 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. Controls ensure the reduction in risk of theft, fraud, and misuse of facilities.			

Control Objective 4 - Environmental Security

Control Objective 4: Controls provide reasonable assurance that physical assets are adequately protected against environmental hazards and related damage.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
4.1	Controls are in place to protect against external and environmental hazards, such as fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster.	Reviewed Disaster Recovery Plan. Interviewed IT Manager. Observed that the computer room is located within the IT office and has biometric locks on the front and rear entrance and it has a separate HVAC system with the temperature set to 65. There is IT Watchdog temperature and humidity sensors which provide email alerts. Observed one alert for the audit period. Observed the following: • The computer room is located on the first floor of a one-story facility and does not have raised floors. The computer room does have a locked door within the secure area and that the three IT personnel, HR, and Operations have a key. • The entire facility has fire and smoke alarms with wet pipe fire extinguishers, including the computer room and smoke and heat detectors tied to the same system. There is no separate fire suppression system in place. Observed the UPS on the servers running at 47% load with a 17-minute run time. The building does not have a generator, but they can send critical jobs to the Speight location facility in Waco within a few miles.	No Relevant Exceptions Noted

Control Objective 4 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that physical assets are adequately protected against environmental hazards and related damage.

Control Objective 5 - Physical Security

Control Objective 5: Controls provide reasonable assurance that physical access to critical applications and data is limited to authorized individuals.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
5.1	Physical security controls are in place for protecting secure areas.	Interviewed Systems Analyst. Observed the following: • The entrance to the facility is controlled via a PIN pad but the main entrance is unlocked during normal business hours. There are no proximity badges but that access to the desktop processing and IT areas is separate enclosed areas with biometric door locks. • The perimeter of the building has intrusion detection alarms and glass breakage sensors that is monitored by ADT. • Employees do not have keys or direct access granted. Observed of 3 of 23 terminated users did not have door access listed on the access list. • There are no colo facilities. Observed the ADT website where user can pull access reports, but not the actual users can be identified. Observed and recorded the visitor logs in other physical security control with no exception noted- KPQ30.	No Relevant Exceptions Noted

5.2	Physical security controls are in place for areas where backup media is stored.	Interviewed IT Manager. Observed that the data center has biometric locks, which can only be accessed by employees in the technology department, HR, COO, and CEO. Observed that there is no backup media storage. There is an AppAssure appliance that mirrors to the drobo and turns over the wire mirrors to the drobo at the colo office facility.	No Relevant Exceptions Noted
5.3	The organization maintains a facility security alarm with an accompanying monitoring agreement.	Reviewed Alarm Contracts. Interviewed IT Manager and Operations Manager. Observed that doors are locked M-F at 5 PM. During this time, the door code is required for access. The security alarm is set by the last person leaving for the night and disarmed by the first person in the morning. The CEO receives a monthly report from the alarm company with all activity. Observed that they have an alarm contract with ADT and it is recurring. Observed that they place reliance on ADT and observed the alarm reporting call tree which includes 4 individuals to include the Operations Manager and the CEO.	No Relevant Exceptions Noted

5.4	The organization has implemented video cameras or other mechanisms for monitoring passage through areas containing sensitive information.	Interviewed Operations Manager. Observed that the organization has ten cameras on the DVR going back to 11/14/17, which is just beyond the 90-day retention period. Observed that some of the interior areas of the warehouse are not fully covered by camera and the quality of the recordings are low. Observed that their current entry system is PIN-based but does not allow a good mechanism for uniquely identifying individuals.	No Relevant Exceptions Noted
5.5	A visitor log is used to document visitor access to secure areas.	Interviewed Systems Analyst. Observed that the visitor log contains: • Visitor name • Firm represented • ID # • Date and time (in/out) • Onsite personnel authorizing physical access Observed logs being retained for over 2 years going back to 2/14/14.	No Relevant Exceptions Noted
Control Objective 5 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that physical assets are adequately protected and that physical access to the computer equipment, system infrastructure, and storage media is limited to authorized personnel.			

Control Objective 6 - Logical Access

Control Objective 6: Controls provide reasonable assurance that logical access to programs, data, and operating systems is restricted to authorized personnel.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
6.1	The organization maintains a policy on access rights and privileges granted to user IDs.	Interviewed Systems Analyst. Reviewed Group Policy screenshot to verify the following settings: • Password History = 3 remembered • Maximum password age = 90 • Minimum password length = 6 characters • Password complexity = enabled • Reversible encryption = disabled	No Relevant Exceptions Noted
6.2	The organization maintains a process for authorizing and implementing user IDs.	Interviewed Systems Analyst. Observed the Active Directory users and groups to verify that all IDs were unique. Observed a user access request form and noted those stored for recently changed user access requests from the prior month (1 of 1). Observed signed and approved access request form from 3 of 28 new hires during the audit period. Reviewed Information Security Policy to verify that privileges are assigned based upon job function and approved by management.	No Relevant Exceptions Noted

6.3	The organization maintains a process for revoking access for terminated/separated employees. Access must be immediately revoked for terminated/separate employees.	Reviewed Information Security Policy to verify that, in the event of termination, HR will notify IT immediately so that the user can be withdrawn from any privileges on the network. The user password and email passwords are changed immediately. For some employees, the account is deleted immediately. For others, files are removed from their accounts as needed, and emails are forwarded for 30 days. After 30 days, their account is re-evaluated. At that time, the account is removed if it is no longer in use. Observed Active Directory for 3 of 22 terminated employees within the audit period to verify that their access had been revoked (either through deleting the account or disablement). Interviewed IT Manager.	No Relevant Exceptions Noted

6.4	The organization maintains a process for authorizing/approving users prior to access.	Reviewed New Employee IT Form. Reviewed Security Groups Change Request Form. Reviewed Information Security Policy to verify that, to provide an employee with new or revised access to AGL systems, a new Employee IT form or a Security Group Change Request Form is filled out and signed by HR, Supervisor, and IT. Privileges are assigned on a need-to-know basis according to job function. Specific privileges are included within these forms. Each user is assigned a unique user ID consisting of their first initial followed by their last name. User is added within Active Directory. Group assignment controls system access rights. Observed signed and approved access request form from 3 of 28 new hires during the audit period. Observed the Active Directory users and groups to verify that all IDs were unique. Interviewed Systems Analyst.	No Relevant Exceptions Noted
6.5	Active Directory provides automated access controls for the organization.	Reviewed Password Complexity Requirements screenshot. Reviewed Account Lockout screenshot. Interviewed IT Manager. Observed that the organization uses Active Directory for the automated access controls.	No Relevant Exceptions Noted

6.6	For online access to services, the organization maintains a process for registering/de-registering users.	Interviewed IT Manager to verify that Integ has a designated person at each facility that has the ability to request access for others. Email is used to ensure that the request is coming from that company. On the SFTP site, the company has one username/password to upload files. This is mainly due to them having automated the process and it is a server connecting and uploading a rather than an individual. Observed the SFTP server where this is one account per company to upload files and that this is mainly an automated process.	No Relevant Exceptions Noted
6.7	Users must be assigned a unique ID before being allowed access to system components.	Reviewed Information Security Policy to verify the use of Active Directory, which enforces unique user IDs. Interviewed IT Manager.	No Relevant Exceptions Noted
6.8	Two-factor authentication is required for remote network access by employees, administrators, and third parties	Interviewed IT Manager. Reviewed Team Viewer document to verify that the following two factors are used: • Something you know - username and password • Something you have – one-time code Observed SpiceWorks and the Team Viewer soft token (one-time use only token) to verify that the above two factors are implemented.	No Relevant Exceptions Noted
Control Objective 6 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that logical access to applications and data is limited to authorized individuals.			

Control Objective 7 - Network Monitoring

Control Objective 7: Controls provide reasonable assurance that network security and monitoring procedures are in place to identify and report unauthorized access attempts.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
7.1	The organization uses SpiceWorks as its network monitoring/logging tool.	Reviewed Local Host text file. Interviewed IT Manager to verify that the company currently has two months of logs. The logs go back to 10/30. Observed that the following, at minimum, are captured: • Source IP • Destination IP • Destination port • Protocol type (ex. TCP, UDP, ICMP) • Timestamp Observed the last two months of logs. Logs cover all critical systems. Observed logs going back to 2014. Reviewed zip file: SpiceWorks Finder Group Scan – All Resources Utilization.	No Relevant Exceptions Noted
7.2	A monthly analysis is performed to monitor system capacity to plan for future requirements.	Reviewed SpiceWorks Alerts screenshot and 2016 Server Analysis spreadsheet, noting that monitors and alerts are set for system disk, memory, and CPU usage. Based upon these reviews, the IT department will tune and/or upgrade systems as needed. Interviewed IT Manager to verify that a monthly manual process is in place whereby they review system capacity and plan for any needed upgrades.	No Relevant Exceptions Noted

7.3	Monitoring is performed to limit information leakage.	Interviewed Systems Specialist and IT Manager to verify the following: • SpiceWorks provides a scan of the network so Integ can view inventory of all hardware, software, applications, and equipment connected to the network. It also detects unwanted devices on the network that may be stealing bandwidth or confidential company information. • SpiceWorks monitors all the network traffic based on the settings created by the administrator. Alerts are set to send details and critical info to key persons at Integ. It also allows the IT staff with full admin rights on Integ systems so they are able to fully manage the network. If an employee is under suspicion, their account can be easily locked, and if someone has locked themselves out, IT can allow them back in. Active Directory can make all changes to any employee's account and protect the integrity of the network. The administrator can use Active Directory software to link devices to a specific user. • If Integ has a large print file, the Systems Specialist will put the file on a thumb drive, walk it over to the printer, then immediately bring the drive back to her desk and format it. The thumb drives are stored in her desk once formatted. Observed that SpiceWorks will alert to network changes. Observed the SpiceWorks console and monitoring events for DLP related items.	Exception Noted

		Exception: This control was implemented while onsite but was not in place long enough to assess its effectiveness. Since USB drives are needed for business operations, disable USB ports on systems that do not need this and enable USB port monitoring on those systems that do. Implement the use of self-encryption drives where thumb drives are needed for business purposes.	
7.4	Sophos provides an intrusion detection/prevention system to detect threats against systems that store, process, or transmit sensitive information.	Interviewed IT Manager to verify that Sophos provides intrusion detection as well as visual alerts to the users and email alerts to IT staff. Their firewall also prevents intrusions by restricting both inbound and outbound traffic according to the rules set up. Reviewed Intrusion screenshot. Observed locked containers around the facility are provided to dispose of confidential customer information. Observed that computers require passwords to prevent anyone from obtaining confidential information. Observed that the IT area has biometric locks to prevent unwanted access to servers and workstations that have administrative rights. Observed that the firewall has the IPS function enabled and licensed until 2/24/17.	No Relevant Exceptions Noted
7.5	SpiceWorks provides the organization's file integrity monitoring solution.	Interviewed IT Manager. Reviewed SpiceWorks Alert screenshot. Observed that Integ uses SpiceWorks to alert of changes to the servers or any system anomalies.	No Relevant Exceptions Noted

Control Objective 7 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that network security and monitoring procedures are in place to identify and report unauthorized access attempts.

Control Objective 8 - Configuration Management

Control Objective 8: Controls provide reasonable assurance that configuration management procedures are in place to identify and report unauthorized changes.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
8.1	The organization tests and approves network changes and changes to firewall and router configurations.	Reviewed Change Request Form to verify that the document is filled out and approved. In systems where there is not a test environment, the config is saved prior to the change so that if a problem is detected, it can immediately be put back to the original configuration. The form captures: • CR # • Department • Date • Location • Phone • Description • Changed needed by date • Reason for change • Request sign off • Approver • Change Type • Change Priority • Environments Impacted • Resources Required • Test Plan Description • Rollback Description • Implementation Test Results Interviewed IT Manager.	No Relevant Exceptions Noted

8.2	Firmware on wireless devices must be updated to support strong encryption	Interviewed IT Manager to verify that Integ does not currently allow open wireless connections on their networks. At corporate, there is a wireless connection for guests, however, this is not on the network. It is a separate ISP connection. It does have encryption and is password protected. Guest wireless is shown on the network diagram. Reviewed Firmware Check email reminder screenshot. Reviewed network diagram to verify that the wireless access point attaches to a separate ISP account not connected the corporate network.	No Relevant Exceptions Noted
8.3	The organization maintains system configuration standards documentation.	Reviewed Workstation Virtual Server Checklist. Reviewed Configuration Standards Policy. Observed that the company has formally documented server workstation install checklists with policy standards to comply with NIST SP 800-123. Additionally, they use MSBA for periodic checking of systems and remediate accordingly. Interviewed IT Manager.	No Relevant Exceptions Noted

8.4	The organization maintains a process for keeping system configuration standards up to date. Action is taken toward regular review of system configuration standards.	Interviewed IT Manager to verify the following: • Servers are subject to standard security management practices which include keeping them up-to-date by applying approved patch management processes. • Antivirus is installed on all devices, including network intrusion detection, on-access scanning, antivirus, and tamper protection. • Active Directory Group Policy is enforced to ensure users change passwords regularly and use a complex password. • Ability to install or remove software is limited to users with administrative privileges. • Software versions are kept up to date and documented through change management network changes. Network topology documentation is maintained. • Action taken toward regular review/updating of system configuration standards would include SpiceWorks Monitoring with alerts about antivirus, software updates and configuration changes. This action is taken by IT staff on a daily basis. Observed the IT daily security task list.	No Relevant Exceptions Noted

8.5	The organization uses industry-accepted hardening standards from NIST SP 800-123 as a basis for system configuration.	Interviewed IT Manager, who explained that NIST SP 800-53 establishes the guidelines to follow in the organization’s Configuration Standards Policy. Integ established the main department responsible for information security along with defining the infrastructure. Additionally, the company established a change management policy that will only allow for changes approved by the IS department. The company also implemented firewalls and security and monitoring standards that permit or deny users access to the system. PCI 2.2 establishes steps to follow to ensure that systems are functional and secure, and systems are continuously monitored and new vulnerabilities are researched. Reviewed Workstation Virtual Server Checklist, a guideline for setting up workstations and servers. This has been modeled of NIST 800-53 and 800-123.	No Relevant Exceptions Noted

8.6	Using security technology websites, Sophos resources, and SpiceWorks resources, personnel with responsibilities for system configurations stay knowledgeable of appropriate ways to securely configure the organization's systems.	Interviewed IT Manager to verify that the following resources are used: • Security technology websites such as TechWorld, NetworkWorld, and SecurityWeek are used. • Personnel follow Sophos presentations and updates on new threats. • The SpiceWorks Community is monitored for latest in network monitoring and threats. • Personnel read appropriate security bulletins available from vendors, user groups, and security institutes. • Personnel ensure that servers are secured physically where no unauthorized person can access them. Interviewed random IT staff onsite to verify their knowledge of secure configurations and to corroborate.	No Relevant Exceptions Noted

8.7	The organization maintains a change management policy.	Reviewed Change Management Process Policy to verify that it captures: • CR # • Department • Date • Location • Phone • Description • Changed needed by date • Reason for change • Request sign off • Approver • Change Type • Change Priority • Environments Impacted • Resources Required • Test Plan Description • Rollback Description • Implementation Test Results Reviewed the following documents: • AppAssure Change document • Phone Update document • ISP Change document Reviewed the last six months of changes, there were three.	No Relevant Exceptions Noted
8.8	Changes that may affect system availability and security are communicated to management and users who may be affected.	Reviewed Change Email screenshots. Interviewed Systems Analyst to verify that, when changes need to be made, a short description of changes scheduled for implementation will be sent by email. Distribution of this email will be to all company's employees including management, change representatives of Integ affiliates, and key business partners.	No Relevant Exceptions Noted

8.9	The organization maintains firewall and router configuration/configuration files.	Interviewed IT Director and outsourced IT Provider. Observed that there are specific rules from the WAN to specific severs on the LAN to try and simulate a DMZ on their flat network but there is not a dedicated DMZ, nor DMZ interface.	No Relevant Exceptions Noted

8.10	Firewalls and routers are configured to limit traffic to that which is necessary for business purposes.	Reviewed SonicWall Access Rules – Speight. Reviewed SonicWall Access Rules. Interviewed Systems Analyst to verify that restrictions are defined on the SonicWall as follows: • Content Filter - Internet Content Filtering equips the SonicWALL to monitor usage and control access to objectionable web content according to established Acceptable Use Policies. • Intrusion Prevention - Intrusion Prevention integrates a high-performance Deep Packet Inspection architecture and dynamically updated signature database to deliver complete network protection from application exploits, worms, and malicious traffic. In addition, Intrusion Prevention provides access control for Instant Messenger (IM) and Peer-to-Peer (P2P) applications. • Gateway Anti-Virus - Gateway Anti-Virus integrates a high performance Real-Time Virus Scanning Engine and dynamically updated signature database to deliver continuous protection from malicious virus threats at the gateway. • Anti-Spyware - Anti-Spyware prevents malicious spyware from infecting networks by blocking spyware installation at the gateway and disrupts background communications from existing spyware programs that transmit confidential data. • RBL Filter - Real-time Black List	No Relevant Exceptions Noted

Control Objective 8 Conclusion: Based on tests of operating effectiveness, the controls described above provide reasonable assurance that configuration management procedures are in place to identify and report unauthorized changes.

Control Objective 9 - Vulnerability Management

Control Objective 9: Controls provide reasonable assurance that systems, processes, and software are tested periodically to ensure that security is maintained over time and after any changes.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
9.1	The organization uses Sophos Enterprise Console to ensure that antivirus software definitions are updated.	Reviewed Sophos screenshot. Interviewed IT Manager. Observed the Sophos console settings: • Frequency of updates is every 30 minutes to the clients; update manager checks 10 minutes. • Agents are set for on access scanning, behavior monitors is enabled. • Agents are password protected to prevent client tampering. Observed logs are retained on the Sophos server for greater than 14 months. Compared the SpiceWorks inventory with systems reporting in the Sophos console to ensure that 100% of systems were reporting and up to date. Observed an email alert from 1/3/16 for three malware and one adware events. All were captured and quarantined. Interviewed System Analyst to verify that she conducted a follow-up investigation and coached the user on security awareness training.	No Relevant Exceptions Noted

9.2	The organization monitors vendors for security patch notifications.	Interviewed IT Manager. Reviewed GPO screenshot. Observed the GPO that checks and downloads updates every day at 3 AM and then prompts users to install and reboot if required for the Windows OS. Server updates are pushed monthly. Reviewed that the client has a monthly task to check for new updates to their critical rasterizing software. Additionally, they are subscribed to newsletters and bulletins from their three main vendors, firewalls, AV auto updates, etc.	No Relevant Exceptions Noted
9.3	The organization complies with legal, regulatory, and/or business requirements for data retention that affect your organization.	Interviewed IT Manager. Reviewed Information Security Policy to verify that at-risk data within the AGL organization is only stored in secured servers or approved data medium(s) within approved areas in the AGL facilities. At-risk data stored in secured servers resides in password-protected partitions with only authorized AGL employee access, on a restricted internal network. In the case of customer at-risk data, the data only remains stored for the duration of the processing of that data or for the required amount of time by the USPS or other authoritative bodies. Customer at-risk data must be removed as soon as allowable. At-risk data is not stored on workstations for any time longer than in-session required accessing or processing. At-risk data is not stored on portable computers at any time. Data files from customers are deleted from the system within one week of receipt.	No Relevant Exceptions Noted

9.4	Sensitive data is secured any time it must be transmitted or received via open, public networks.	Reviewed Certificate for SFTP. Reviewed SSL Server Test Upload – Integ Does. Reviewed SSL Certificate. Reviewed the SSL Labs report with an A- score with a chain issue identified. Observed SHA256bit with RSA certification. Interviewed IT Manager.	No Relevant Exceptions Noted
9.5	Vendor recommendations and best practices underpin the organization's encryption methods for open transmission of sensitive data.	Reviewed Certificate for SFTP connections. Reviewed SSL Server Test Upload – Integ Does (SSL Labs report). Reviewed the SSL Labs report with an A- score with a chain issue identified. Observed SHA256bit with RSA certification. Interviewed IT Manager.	No Relevant Exceptions Noted
9.6	Information involved in application service transactions is protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay	Interviewed IT Manager to verify that Integ uses record counts to validate that all records are processed. Observed the record count report to ensure processing integrity. Reviewed the following: • Nice Count in Integ System screenshot • Notice Count from Bank screenshot	No Relevant Exceptions Noted
Control Objective 9 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that systems, processes, and software are tested periodically to ensure that security is maintained over time and after any changes.			

Control Objective 10 - Backup and Restoration

Control Objective 10: Controls provide reasonable assurance that backups of data and system files are regularly created and that archived data is available for restoration in the event of processing errors.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
10.1	The organization maintains backup policies and procedures.	Reviewed Data Backup and Storage Policy. Interviewed System Analyst. Observed the following: • The type of backups performed are base image first then incremental snapshots. • The Dell AppAssure is backed up. Backups are disk-to-disk. • The AppAssure appliance is onsite at Integ. Critical data is backed up from the AppAssure appliance to an external hard drive appliance (Drobo). From there, this data is replicated to the offsite facility at 4500 Speight and a similar external hard drive appliance. • The backup appliance is checked daily to verify there are no errors and monthly a test is performed to restore files from the repository.	No Relevant Exceptions Noted

Control Objective 10 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that backups of data and system files are regularly created and that archived data is available for restoration in the event of processing errors.

Control Objective 11 - Business Continuity and Disaster Recovery

Control Objective 11: Controls provide reasonable assurance that the organization maintains controls which allow for function to continue in the event of a security incident.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
11.1	Plans are in place to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	Reviewed Integ Disaster Recovery document, which includes: • General Information • Scope of Disaster Recovery Plan • Risk Assessments • Operational Priorities • Redundant Off-Site Locations • Disaster Recovery Procedures Observed that a list of inventory and critical components are in SpiceWorks and that redundancy between sites is in place for the banking clients that are the scope of this audit. Observed the notification teams and call trees. Restoration procedures are via virtual machines where the data is replicated from the drobo recovery boxes at the primary and colo location. Observed that management approved and participates in the plan. The DRP will be called by the Operations Manager or Owner. Annually, tabletop exercises are conducted and issues identified are added to the plan as evidenced by the revision history. Interviewed IT Manager.	No Relevant Exceptions Noted

11.2	The organization ensures that the business continuity plans are tested and updated.	Reviewed Disaster Recovery Exercise. Interviewed IT Manager. Observed that the company formally documents results and lessons learned. There were no identified deficiencies in this exercise and so no updates were made to the plan. This is tested annually in the last quarter of the year using tabletop exercises.	No Relevant Exceptions Noted
Control Objective 11 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that the organization maintains controls which allow for function to continue in the event of a security incident.			

Integ

Type I Service Organization Control Report (SOC 2)

Independent Report on a Description of a Service Organization’s System and the Suitability of the Design of the Controls to meet the criteria for the Security and Confidentiality principles as of January 31, 2017.

Kirkpatrick Price, LLC
1228 East 7th Ave., Suite 200
Tampa, FL 33605

TABLE OF CONTENTS

MANAGEMENT OF INTEG’S ASSERTION REGARDING ITS TRANSACTIONAL PRINTING SYSTEM AS OF JANUARY 31, 2017

INTEG'S ASSERTION

We have prepared the attached description titled "Description of Integ's transactional printing system As of January 31, 2017" (the description), based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system in paragraphs 1.34-.35 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2^{SM})* (the description criteria). The description is intended to provide users with information about the transactional printing system, particularly system controls intended to meet the criteria for the Security and Confidentiality principles set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that

a) The description fairly presents the transactional printing system as of January 31, 2017, based on the following description criteria:
   i. The description contains the following information:
      1. The type of services provided
      2. The components of the system used to provide the services, which are the following:
         - *Infrastructure*. The physical and hardware components of a system (facilities, equipment, and networks).
         - *Software*. The programs and operating software of a system (systems, applications, and utilities).
         - *People*. The personnel involved in the operation and use of a system (developers, operators, users, and managers).
         - *Procedures*. The automated and manual procedures involved in the operation of a system.
         - *Data*. The information used and supported by a system (transaction streams, files, databases, and tables).
      3. The boundaries or aspects of the system covered by the description
      4. How the system captures and addresses significant events and conditions, other than transactions.
      5. The process used to prepare reports or other information provided to user entities of the system.
      6. If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization or other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls
      7. For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system
      8. For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or

in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria; and for privacy, the types of activities that the subservice organization would need to perform to comply with our privacy commitments

9. Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore
10. Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b) The controls stated in the description were suitably designed as of the specified date to meet the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR’S REPORT

on a Description of a Service Organization’s System
and the Suitability of the Design of the Controls

INDEPENDENT SERVICE AUDITOR'S REPORT

David Anderton, President and CEO
Integ
700 W. Loop 340
Waco, Texas 76710

Scope

We have examined the attached description titled "Description of Integ's transactional printing system As of January 31, 2017" (the description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the Security and Confidentiality set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), as of January 31, 2017. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Integ's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

Integ uses Xerox to perform high volume printer services. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The description presents Integ's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet certain applicable trust services criteria. The description does not include any of the controls implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization or the subservice organization's compliance with the commitments in its statement of privacy practices.

Service Organization's Responsibilities

Integ has provided the attached assertion titled "Management of Integ's Assertion Regarding Its transactional printing system As of January 31, 2017," which is based on the criteria identified in management's assertion. Integ is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of the description and assertions; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in Integ's assertion and on the suitability of the design of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed to meet the applicable trust services criteria as of January 31, 2017.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design of those controls to meet the applicable trust services criteria. Our procedures include assessing the risks that the description is not fairly presented and that the controls were not suitably designed to meet the applicable trust services criteria. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria identified in Integ's assertion and the applicable trust services criteria

a) the description fairly presents the system that was designed and implemented as of January 31, 2017.

b) the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively as of January 31, 2017, and user entities applied the complementary user-entity controls contemplated in the design of Integ's controls as of January 31, 2017.

Restricted Use

This report, is intended solely for the information and use of Integ; user entities of Integ as of January 31, 2017; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties
- Internal control and its limitations
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

CPA

Damon Sullivan, CPA
KirkpatrickPrice, LLC
1228 East 7th Ave. Suite 200
Tampa, FL 33605

February 15, 2017

INTEG'S DESCRIPTION OF ITS TRANSACTIONAL PRINTING SYSTEM AS OF JANUARY 31, 2017

SYSTEM OVERVIEW

Background

The Anderton Group began in June of 1994 with the purchase of Brazos Printing. Over the next several years, sales doubled due to customer commitment and the quality of the company's products and services.

In 1996, the company took a new step with the acquisition of Cen-Plex Mailing, a 24-year veteran of the mailing business.

Next came Gatesville Printing, then Prim's Mailing Center. Through innovation and equipment enhancements, The Anderton Group became a leader in the full-service mailing industry.

2001 brought the purchase of a manufacturing facility large enough to house the company's growing mailing operations. By this time, a name change was needed to represent the company's capabilities, and MailMax Direct began its life.

Additional acquisitions to Anderton Group over the past few yours included Direct Mail Partners in Tyler Texas, PMP Printing in Temple, Texas and the latest being Central Texas Printing in Waco, Texas. These acquisitions strengthened the services position within Anderton Group.

Now, Integ brings full integration of data, print, and mail capabilities, as well as traditional and digital marketing muscle, to our ever-growing client roster, while maintaining the highest integrity to both our clients and employee family.

INFRASTRUCTURE

Software

The organization maintains an inventory of critical software:

- SonicWall
- SpiceWorks
- CrushFTP
- AppAssure

The organization does not perform software development.

People

The following individuals comprise the company's management team:

- David Anderton – President/CEO
- David Christian – Production Manager
- Chuck White – Production Manager
- Brandon Biggs – First Class Mail Manager
- Phil Roach – Sales/Customer Service Manager
- Teresa Mosley – Facilities Management

Procedures

The following processes and procedures are maintained:

- Change Management Process Policy
- Computer and Internet Policy
- Configuration Standards
- Configuration Standards Policy
- Credit Card Policy
- Daily Security Procedures
- Data Backup and Storage Policy
- Disaster Recovery Plan
- Documentation Retention Policies and Procedures
- Electronic Data Retention Policy
- ID Badge Policy
- Incident Response Plan and Procedure
- Information Security Policy
- Internet and Computer Usage Policy
- Key Policy
- Locker Policy
- Lockout Policy
- Network Scanning Evaluation and Remediation Process
- Security Incident Procedures
- Security Policy
- Travel Policy

Data

Integ receives sensitive data that includes bank statement info such as bank account numbers and amounts, insurance policy information, and information for utility bills. This data is stored, transmitted, and processed in a variety of formats, including PDF, PCL, .txt, .csv, .xls.

At-risk data within the AGL organization is only stored on secure servers or approved data medium(s) within approved areas in the AGL facilities. At-risk data stored in secured servers resides in password protected partitions with only authorized AGL employee access, on a restricted internal network. In the case of customer at-risk data, the data only remains stored for the duration of the processing of that data or for the required amount of time by the USPS or other authoritative bodies. Customer at-risk data must be removed as soon as allowable. At-risk data is not stored on workstations for any time longer than in-session required accessing or processing. At-risk data is not stored on portable computers at any time. Data files from customers are deleted from the system within one week of receipt.

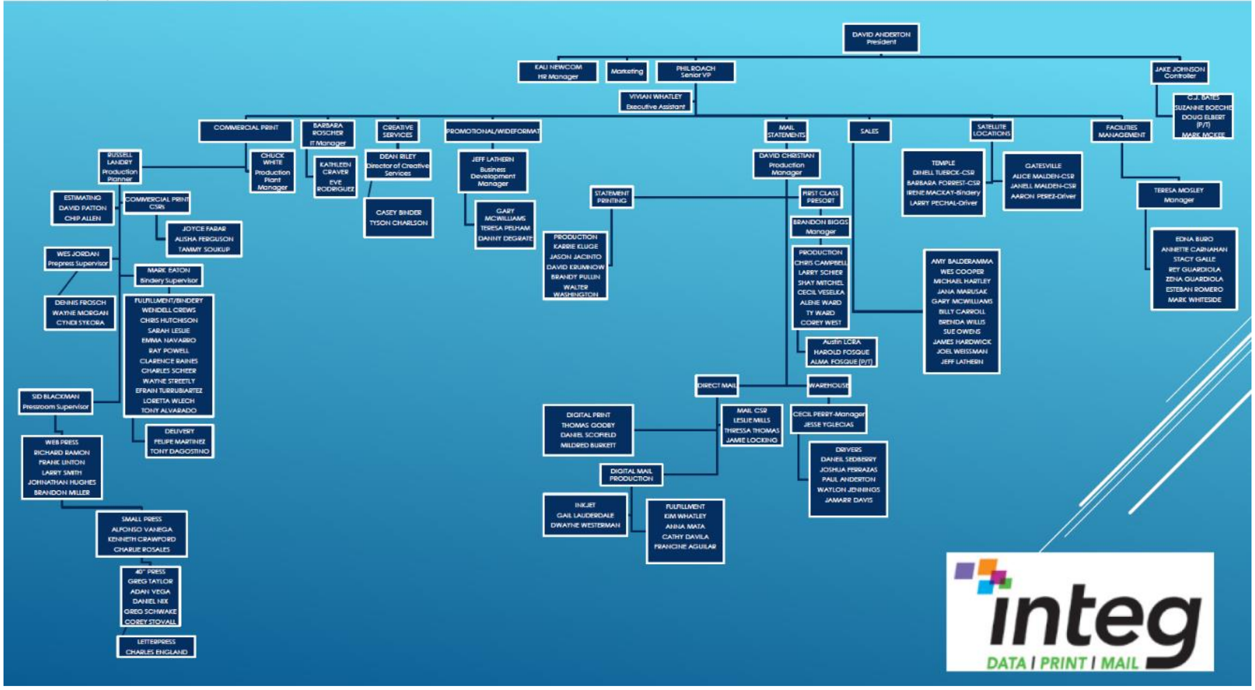
If PHI documents are uploaded to Integ's servers, Integ asks the customer to give them a count of the uploaded documents. Integ then verifies the number of documents processed against the customer's number. If there are any discrepancies, the documents are held until the matter is resolved.

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring of Controls

Control Environment

Management Philosophy

An organization chart is maintained to highlight the division of responsibility within the company:


DAVID ANDERTON President
KALI NEWCOM HR Manager
Marketing
PHIL ROACH Senior VP
JAKE JOHNSON Controller
C.J. BATES SUZANNE BOECHE DOUG ELBERT (P/T) MARK MCKEE
VIVIAN WHATLEY Executive Assistant
COMMERCIAL PRINT
BARBARA ROSCHER IT Manager
CREATIVE SERVICES
PROMOTIONAL/WIDEFORMAT
MAIL STATEMENTS
SALES
SATELLITE LOCATIONS
FACILITIES MANAGEMENT
RUSSELL LANDRY Production Planner
CHUCK WHITE Production Plant Manager
KATHLEEN CRAVER EVE RODRIGUEZ
DEAN RILEY Director of Creative Services
CASEY BINDER TYSON CHARLSON
JEFF LATHERN Business Development Manager
GARY MCWILLIAMS TERESA PELHAM DANNY DEGRATE
ESTIMATING DAVID PATTON CHIP ALLEN
COMMERCIAL PRINT CSRs
JOYCE FARAR ALISHA FERGUSON TAMMY SOUKUP
WES JORDAN Prepress Supervisor
DENNIS FROSCH WAYNE MORGAN CYNDI SYKORA
MARK EATON Bindery Supervisor
FULFILLMENT/BINDERY WENDELL CREWS CHRIS HUTCHISON SARAH LESLIE EMMA NAVARRO RAY POWELL CLARENCE RAINES CHARLES SCHEER WAYNE STREETLY EFRAIN TURRUBIARTEZ LORETTA WLECH TONY ALVARADO
SID BLACKMAN Pressroom Supervisor
DELIVERY FELIPE MARTINEZ TONY DAGOSTINO
WEB PRESS RICHARD RAMON FRANK LINTON LARRY SMITH JOHNATHAN HUGHES BRANDON MILLER
SMALL PRESS ALFONSO VANEGA KENNETH CRAWFORD CHARLIE ROSALES
40" PRESS GREG TAYLOR ADAN VEGA DANIEL NIX GREG SCHWAKE COREY STOVALL
LETTERPRESS CHARLES ENGLAND
STATEMENT PRINTING
PRODUCTION KARRIE KLUGE JASON JACINTO DAVID KRUMNOW BRANDY PULLIN WALTER WASHINGTON
DAVID CHRISTIAN Production Manager
FIRST CLASS PRESORT
BRANDON BIGGS Manager
PRODUCTION CHRIS CAMPBELL LARRY SCHIER SHAY MITCHEL CECIL VESELKA ALENE WARD TY WARD COREY WEST
Austin LCRA HAROLD FOSQUE ALMA FOSQUE (P/T)
DIRECT MAIL
WAREHOUSE
DIGITAL PRINT THOMAS GODBY DANIEL SCOFIELD MILDRED BURKETT
MAIL CSR LESLIE MILLS THRESSA THOMAS JAMIE LOCKING
CECIL PERRY-Manager JESSE YGLECIAS
DRIVERS DANEIL SEDBERRY JOSHUA FERRAZAS PAUL ANDERTON WAYLON JENNINGS JAMARR DAVIS
DIGITAL MAIL PRODUCTION
INKJET GAIL LAUDERDALE DWAYNE WESTERMAN
FULFILLMENT KIM WHATLEY ANNA MATA CATHY DAVILA FRANCINE AGUILAR
TEMPLE DINELL TUERCK-CSR BARBARA FORREST-CSR IRENE MACKAY-Bindery LARRY PECHAL-Driver
GATESVILLE ALICE MALDEN-CSR JANELL MALDEN-CSR AARON PEREZ-Driver
AMY BALDERAMMA WES COOPER MICHAEL HARTLEY JANA MARUSAK GARY MCWILLIAMS BILLY CARROLL BRENDA WILLIS SUE OWENS JAMES HARDWICK JOEL WEISSMAN JEFF LATHERN
TERESA MOSLEY Manager
EDNA BURO ANNETTE CARNAHAN STACY GALLE REY GUARDIOLA ZENA GUARDIOLA ESTEBAN ROMERO MARK WHITESIDE
integ
DATA | PRINT | MAIL

Security and Confidentiality Management

Management's communication sets the tone and direction for the entire company. Security training is conducted on an annual basis. The organization maintains a principle called "Integ Way" that guides operational procedures. The Integ Way places focus on organization excellence and client experience.

Security and Confidentiality Policies

The organization maintains a process for reviewing policies. The review process is completed by multiple managers and senior leadership and ultimately approved by the President/CEO. The policy is reviewed annually.

Controls Related to Personnel

The organization maintains an employee handbook that is printed and shared with new hires and all employees annually. The handbook is distributed sooner if there is a change and re-acknowledgement is required. The handbook covers:

- Code of Conduct
- Ethics

- Reference Checks
- Discipline

Security Policies

Physical and Environmental Security

Physical security controls are in place to protect secure areas. After hours, employees must have a key code to get into the facility as well as a code to turn off the alarm system. Alarm codes and key codes are immediately changed when personnel are terminated. Any visitors must sign in before entering the facility. All visitors must be accompanied by an AGL employee. Biometric locks are used for the IT department. Locked containers are used for PHI information that will be shredded at a later date.

Doors are locked Monday-Friday at 5 PM. During this time, individuals must use the door code to gain access. The security alarm is set by the last person leaving for the night and disarmed by the first person in the morning. The CEO receives a monthly report from the alarm company with all activity.

Security cameras cover each of the entrances into the building. The organization also maintains cameras that display areas within the facility that might contain sensitive information. Ten cameras are maintained and the DVR retains camera footage for at least 90 days.

The organization maintains a visitor log. Visitors are required to sign the visitor log at the reception desk. The logs contain the following information:

- Visitor name
- Data
- Time in
- Time out
- Reason/business name
- Escorted by

The organization has implemented environmental controls. The computer room is located within the IT office and has biometric locks on the front and rear entrance along with a separate HVAC system with the temperature set to 65. IT Watchdog temperature and humidity sensors are in place and provide email alerts.

The computer room is located on the first floor of a one-story facility and does not have raised floors. The entire facility has fire and smoke alarms with wet pipe fire extinguishers, including the computer room and smoke and heat detectors tied to the same system.

Change Management

A change management process is in place. The process captures:

- CR #
- Department
- Date

- Location
- Phone
- Description
- Changed needed by date
- Reason for change
- Request sign off
- Approver
- Change type
- Change priority
- Environments impacted
- Resources required
- Test plan description
- Rollback description
- Implementation test results

The organization maintains a process for testing and approving network changes. A change request form is filled out and approved. In systems where there is not a test environment, the config is saved prior to the change so that if a problem is detected, it can immediately be put back to the original configuration.

Systems are configured with the latest patches and software updates along with antivirus protection. Group Policy is configured for complex passwords. SpiceWorks monitors and scans the network daily for any changes or additions to the network. An email alert is sent the IT department when there have been additions so they may be verified. Any systems added to the network must go through the change management process and will be verified that it meets Integ criteria. Integ has established a workstation and server install checklist to make sure the criteria is met.

Servers are subject to standard security management practices which include keeping them up-to-date by applying the approved patch management processes. Antivirus is installed on all devices, which includes network intrusion detection, on-access scanning, and antivirus and tamper protection. The ability to install or remove software is limited to users with administrative privileges. Software versions are kept up to date through the change management network changes. Network topology documentation is maintained.

Hardening standards are based on NIST SP 800-53. The main department is responsible for information security along with defining the infrastructure. Integ has implemented firewalls and security and monitoring standards that permit or deny users access to the system. Patches are applied as necessary. Service accounts that are not used are removed or disabled. Unnecessary software is removed from servers and workstations.

Personnel with responsibilities for system configuration stay knowledgeable of appropriate ways to securely configure the organization's systems:

- Security technology websites such as TechWorld, NetworkWorld, and SecurityWeek are used.

- Personnel follow Sophos presentations and updates on new threats.
- The SpiceWorks Community is monitored for latest in network monitoring and threats.
- Personnel read appropriate security bulletins available from vendors, user groups, and security institutes.
- Personnel ensure that servers are secured physically where no unauthorized person can access them.

Changes that may affect system availability and system security are communicated to management and users who may be affected. When changes need to be made, a short description of changes scheduled for implementation is sent by email. This email is distributed to all Integ employees (including management), change representatives of affiliates, and key business partners.

Firewalls and routers are configured to limit traffic to that which is necessary for business purposes. The restrictions are defined on the SonicWALL as follows:

- Content Filter - Internet Content Filtering equips the SonicWALL to monitor usage and control access to objectionable web content according to established Acceptable Use Policies.
- Intrusion Prevention - Intrusion Prevention integrates a high-performance Deep Packet Inspection architecture and dynamically updated signature database to deliver complete network protection from application exploits, worms, and malicious traffic. In addition, Intrusion Prevention provides access control for Instant Messenger (IM) and Peer-to-Peer (P2P) applications.
- Gateway Anti-Virus - Gateway Anti-Virus integrates a high performance Real-Time Virus Scanning Engine and dynamically updated signature database to deliver continuous protection from malicious virus threats at the gateway.
- Anti-Spyware - Anti-Spyware prevents malicious spyware from infecting networks by blocking spyware installation at the gateway and disrupts background communications from existing spyware programs that transmit confidential data.
- RBL Filter - Real-time Black List

System Monitoring

The organization maintains network monitoring/logging processes. SpiceWorks actively scans network devices, including workstations, servers, printers, etc. It provides and manages alerts on the following items:

- Equipment
- HelpDesk Tickets issued by employees
- A timeline of tickets and other network events
- Details on Antivirus (Sophos) versions, installations, and updates
- An inventory summary with equipment details
- Software patches with priority

This information and reports are accessed by IT Personnel only. Reporting data cannot be modified.

The organization maintains a process to monitor system capacity and plan for future requirements. Integ performs a monthly analysis on its servers. When the company notices that it is below 10% free space on servers, IT takes steps to see if more space can be allocated. If not, then Integ makes plans to add more drives or replace equipment. Integ also receives notices from SpiceWorks if a volume goes below 10% free space.

Monitoring is performed to limit information leakage. SpiceWorks provides a scan of the network so Integ can view inventory of all hardware, software, applications, and equipment connected to the network. SpiceWorks also detects unwanted devices on the network that may be stealing bandwidth or confidential company information. Regular scans allow Integ to eliminate internal equipment theft and also detect malfunctions before they deal permanent damage.

Sophos provides intrusion detection as well as visual alerts to the users and email alerts to IT staff. The firewall also prevents intrusions by restricting both inbound and outbound traffic according to the rules set up. Locked containers are provided to dispose of confidential customer information. Computers require passwords to prevent anyone obtaining confidential information. IT area has biometric locks to prevent unwanted access to servers and workstations that have administrative rights.

Problem Management

The organization maintains incident response policies and procedures. The following steps are taken:

1. Incident Identification
2. Reporting and Incident Declaration Procedures
3. Incident Severity Classification
    a. Level 1 - One case of potentially harmful activity
    b. Level 2 - One definite example of harmful activity or multiple examples of potentially harmful activity
    c. Level 3 - Major attempted or successful security breach or multiple examples of harmful activity
4. Typical Response Procedures
5. Root Cause Analysis and Lessons Learned
6. Plan Testing and Training
7. Critical Systems Restore Strategy

Data Backup and Recovery

The organization maintains backup policies and procedures. The following controls are in place for backup procedures:

- IT staff are responsible for ensuring that backup copies of all confidential information on Integ electronic media and information systems are made regularly. This includes both confidential information received by Integ and created within Integ. Information systems and electronic media include file servers, database servers, and Domain Controllers and web servers.
- IT staff are responsible for ensuring that Integ has adequate backup systems that ensure the ability to create and recover data following a disaster or intentional destruction of

data or equipment failure. Specific data must be stored at a remote location that is a sufficient distance from Integ facilities to escape damage from a disaster at Integ.

- IT staff are responsible for ensuring that backup copies of information stored at secure remote locations are accessible to authorized Integ employees for timely retrieval of the information.
- IT staff are responsible for ensuring that backup media containing information at the remote backup storage site is given an appropriate level of physical and environmental protection consistent with the standards applied to information physically at Integ.
- Backup and restoration procedures for Integ electronic media and information systems containing information must be regularly tested by IT staff or designee to ensure that they are effective and that they can be completed within a reasonable amount of time.
- The retention period for backup of information on Integ information systems and any requirements for archive copies to be permanently retained must be defined and documented by the Information Security Officer.

The organization maintains a business continuity/disaster recovery plan that covers the following items:

- Scope of Disaster Recovery Plan
    - List of Operations Covered
    - Operation Detail
- Risk Assessments
    - Natural Disaster/Emergency Definitions
    - Technical Disaster/Emergency Definitions
    - Human Emergency/Threat Definitions
    - Failure Scenario Impact Analysis
- Operational Priorities
    - Critical Operations
    - Critical Operational Personnel
    - Critical Equipment
    - Critical Applications
    - Critical Data
    - Critical Documents / Materials
- Redundant Off-Site Locations
    - Off-Site Locations
    - Redundant Operations
    - Redundant Equipment
    - Third-Party Equipment Support
- Disaster Recovery Procedures
    - Safety Issues
    - Disaster Recovery Triggers
    - Disaster Notification
    - Disaster Recovery Activation
    - Damage Assessment
    - Equipment Protection and Salvage
    - Emergency Procurement Procedure
    - Off-Site Preparations

  - Operational Priority Review
  - Individual Service Continuity Procedures
  - Processing Cycle and Reporting
  - Returning to Normal Operations

System Account Management

The organization maintains a policy on access rights and privileges granted to user IDs. User IDs are based on the user's first initial and last name. A new employee IT form is filled out and signed by HR, Supervisor, and IT. Privileges are assigned according on a need-to-know basis according to job function. Active Directory is used as the organization's automated access control system. Two-factor authentication is used for secure login.

Access to server partitions is only granted to authorized AGL employees using approved internal software on approved workstations on the AGL premises. Access is controlled by authorized AGL IT administrators. Short term access of at-risk data such as workstation client access operations is limited to each in-use session by an authorized AGL employee on a workstation approved for such access by AGL IT administrators within the AGL premises.

In the event of termination of an employee, HR notifies IT immediately so that the user can be withdrawn from any privileges on the network. The user password and email passwords are changed immediately. For some employees, the account is deleted immediately. For others, files are removed from their accounts as needed, and emails are forwarded for 30 days. After 30 days, their account is re-evaluated. At that time, the account is removed if it is no longer in use.

AGL employee user accounts and passwords are controlled by authorized AGL administrators. Passwords must be changed every six months. User accounts and passwords control access to network partitions, workstations, servers, and other services and applications.

The organization maintains a process for registering/de-registering users for online access to services. On the SFTP site, the company has one username/password to upload files. This is mainly due to them having automated the process and it is a server connecting and uploading a rather than an individual.

Risk Assessment Process

The organization maintains a risk analysis policy as a guideline when accepting risk. This standard is based on:

- National Institute of Standards and Technology (NIST) Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems"
- National Institute of Standards and Technology (NIST) Special Publication 800-14, "Risk Management Guide for Information Technology Systems"
- National Institute of Standards and Technology (NIST) Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems"

The organization maintains a risk assessment matrix that accounts for the following:

- Priority of the Risk
    - Low
    - Moderate
    - High
    - Extreme
- Consequences
    - Insignificant
    - Minor
    - Moderate
    - Major
    - Catastrophic
- Likelihood
    - Almost certain to occur in most circumstances
    - Likely to occur frequently
    - Possible and likely to occur at some time
    - Unlikely to occur but could happen
    - May occur but only in rare and exceptional circumstances

Information and Communication Systems

The organization maintains an information security policy to govern the operating environment. The policy is reviewed at least once annually and covers legal, regulatory, and industry standards. Responsibilities for information security is reinforced in an annual security awareness training program.

The organization distributes the information security policy to personnel and business partners. Each policy administrator has a pdf copy of the policy that can be printed or emailed as requested by existing employees or business partners. A paper copy is distributed in the new employee packet as well as signed off and given to employees yearly. An NDA is signed any external party before sharing any sensitive information.

The organization maintains a process whereby users are provided a process for informing the organization about security breaches and for submitting complaints. In the event that a customer, data owner, IT personnel, or Information Technology Services representative identifies a potential security incident involving a computer, the computer must first be disconnected from the network, then shutdown. In all instances, the Operating Unit awaits further instructions prior to continued operation of the computer.

Any employee or data owner who believes that a security incident has occurred must immediately notify their supervisor, HR, or any IT personnel. There is also a suggestion box outside of the HR Office that can be used in situations where the person reporting wants to remain anonymous. Upon notification by an employee, IT personnel promptly handle the incident according to the incident response and procedure policy.

In the event of loss or theft of customer materials or mailpieces, the customer owning those items is also notified by contacting either the primary customer lead contact or contacts specified in any contract or contact list with the customer. Internal complaints can be made directly to a supervisor, HR, IT department or in the suggestion box located outside of the HR office.

Monitoring Controls

Monitoring activities are performed by management to ensure operational quality and control. An Integ Error report process is in place. When an error is made, the manager calculates how much the error costs in time and paper, then they sit down with the employee and go over the report and the cost. The files are kept and if the same employee continues to make errors, then write ups are conducted.

Management staff routinely perform a review of the status of each processing workstation system. The review process looks for the condition of each customer account folder, data files, or other abnormalities. Management staff performs random auditing of customer data processing by Integ operators. Random audits occur physically next to the operator as the operation performs tasks. These audits look for errors in processing, deviations from standard procedures, and other abnormalities in processing.

Management staff perform code review and process review on the components of each customer application submitted to be placed in live production state. In order for a customer application to be placed in live production state, the customer application must be approved by these review processes. These reviews look for accuracy of customer data, security of the customer data, abnormalities which could potentially cause errors or accidental or purposeful exposures of or changes to data.

In the event that any of these control methods raises an issue, an attempt is made to correct the issue. If possible, supervisors offer more training and reprimand the operator is necessary.

Applicable Trust Services Criteria and Related Controls

The following sections and their accompanying tables outline the criteria and related controls for each Trust Services Principle applicable to Integ's transactional printing system.

Criteria Common to All Security and Confidentiality Principles

1.0 Common Criteria Related to Organization and Management

Control #	Control Activity
1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they relate to Security and Confidentiality.
1.1.1	The organization maintains a clearly defined organizational structure.
1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and placed in operation.
1.2.1	Monitoring activities—including the use of error documentation—are performed to ensure operational quality and control.
1.2.2	A review process is in place by management for creating, approving, and maintaining the organization's policies.
1.3	Personnel responsible for designing, developing, implementing, operating, maintaining and monitoring the system affecting Security and Confidentiality have the qualifications and resources to fulfill their responsibilities.
1.3.1	Training programs have been implemented by the organization.
1.3.2	The organization ensures that personnel with responsibilities for system configurations stay knowledgeable of appropriate ways to securely configure the organization's systems.
1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to Security and Confidentiality.
1.4.1	Hiring and termination policies are in place and include background checks and onboarding/offboarding checklists.
1.4.2	The organization maintains an employee handbook that outlines HR policies.
1.4.3	The organization maintains a process for conducting background checks.

Control #	Control Activity
1.4.4	The organization maintains onboarding documentation covering company disclosures and management expectations.

2.0 Common Criteria Related to Communications

Control #	Control Activity
2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.
2.1.1	The organization maintains marketing and/or contractual materials that describe the services or scope of work provided to clients.
2.2	The entity's Security and Confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.
2.2.1	The organization ensures that security policies define information security responsibilities for all personnel.
2.3	The entity communicates the responsibilities of internal and external users and others whose roles affect system operation.
2.3.1	Job descriptions are maintained for critical functions in the organization.
2.4	Internal and external personnel with responsibility for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the Security and Confidentiality of the system, have the information necessary to carry out those responsibilities.
2.4.1	Training programs have been implemented by the organization.
2.4.2	The organization ensures that personnel with responsibilities for system configurations stay knowledgeable of appropriate ways to securely configure the organization's systems.
2.5	Internal and external system users have been provided with information on how to report Security and Confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.
2.5.1	The organization ensures that training is given to personnel with security breach responsibilities.
2.5.2	A process is in place whereby clients and/or users are provided a process for informing the organization about security breaches and for submitting complaints.
2.5.3	The organization maintains incident response policies and procedures.

Control #	Control Activity
2.6	System changes that affect internal and external system user responsibilities or the entity’s commitments and requirements relevant to Security and Confidentiality are communicated to those users in a timely manner.
2.6.1	Changes that may affect system availability and system security are communicated to management and users who may be affected

3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls

Control #	Control Activity
3.1	The entity (1) identifies potential threats that would impair system Security and Confidentiality commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies).
3.1.1	The organization maintains a process for selecting controls that transfer, avoid, or mitigate risk.
3.1.2	The organization maintains an annual risk assessment process using NIST 800-14 and 800-18 guidance.
3.2	The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.
3.2.1	The organization maintains an information security policy that covers legal, regulatory, and industry standards.
3.3	The entity (1) identifies and assesses changes (for example, environmental, regulatory, and technological changes) that could significantly affect the system of internal control for Security and Confidentiality and reassesses risks and mitigation strategies based on the changes and (2) reassesses the suitability of the design and deployment of control activities based on the operation and monitoring of those activities, and updates them as necessary.
3.3.1	The organization maintains a change management policy that guides the change process.

4.0 Common Criteria Related to Monitoring of Controls

Control #	Control Activity
4.1	The design and operating effectiveness of controls are periodically evaluated against Security and Confidentiality commitments and requirements, corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.
4.1.1	Daily operational security procedures are performed to check for any potential security issues.

5.0 Common Criteria Related to Logical and Physical Access Controls

Control #	Control Activity
5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction od authorized user access to system components, or portions thereof, authorized by management, including, hardware, data, software, mobile, devices, output, and offline elements; and (3) prevention and detection of unauthorized access.
5.1.1	Active Directory is used as the company’s automated access control system.
5.2	New internal and external system users are registered and authorized prior to being issued system credentials, and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.
5.2.1	The organization maintains an inventory of system users, groups, and domain policies.
5.2.2	The organization maintains a process for approving/authorizing users prior to access.
5.3	Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data).
5.3.1	The organization ensures that users must be assigned a unique ID before being allowed access to system components.
5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them.
5.4.1	The organization maintains a policy on access and rights granted to user IDs.
5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel.
5.5.1	Physical controls—such as biometric locks, keypad locks, intrusion alarms, badges, and cameras—are in place for protecting secure areas.
5.6	Logical access security measures have been implemented to protect against Security and Confidentiality threats from sources outside the boundaries of the system.
5.6.1	Multi-factor authentication is required for remote network access by employees.

Control #	Control Activity
5.7	The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to Security and Confidentiality.
5.7.1	Vendor recommendations and best practices underpin the organization's encryption methods for open transmission of sensitive data.
5.7.2	Information involved in application service transactions is protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, and unauthorized message duplication or replay.
5.8	Controls have been implemented to prevent of detect and act upon the introduction of unauthorized or malicious software.
5.8.1	Sophos Enterprise Console is used to ensure that antivirus software definitions are updated.

6.0 Common Criteria Related to System Operations

Control #	Control Activity
6.1	Vulnerabilities of system components to Security and Confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities.
6.1.1	SpiceWorks is used as the organization's network logging/monitoring tool.
6.1.2	The organization maintains documentation from responded-to security incidents or alerts.
6.1.3	Sophos provides intrusion detection/prevention systems to detect threats against systems that store, process or transmit sensitive information.
6.2	Security and Confidentiality incidents, including logical and physical security breaches, failures, concerns, and other complaints, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures.
6.2.1	The organization maintains incident response policies and procedures.
6.2.2	The organization maintains documentation from responded-to security incidents or alerts.

7.0 Common Criteria Related to Change Management

Control #	Control Activity
7.1	Security and Confidentiality commitment and requirements are addressed, during the system development lifecycle including design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.
7.1.1	The organization maintains hardening standards as a basis for system configuration standards. The hardening standards are based on NIST SP 800-123.
7.2	Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the system commitments and requirements as they relate to Security and Confidentiality.
7.2.1	The organization maintains a process for keeping system configuration standards up to date.
7.2.2	The organization ensures that the information security policy is reviewed and updated.
7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.
7.3.1	The organization deploys the change management process when deficiencies are discovered.
7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with Security and Confidentiality commitments and requirements.
7.4.1	The organization ensures that the change management process is reviewed.

Additional Criteria for Confidentiality

Control #	Control Activity
1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes in accordance with confidentiality commitments and requirements.
1.1.1	The organization's security policies define information security responsibilities for all personnel.
1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, disclosure during input, processing, retention, output, and disposition in accordance with confidentiality commitments and requirements.
1.2.1	The organization has implemented privacy policies for handling personal information in accordance with relevant legislation and regulations.
1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties in accordance with confidentiality commitments and requirements.
1.3.1	Sensitive data is secured any time it must be transmitted or received via open, public networks.
1.4	The entity obtains confidentiality commitments that are consistent with the entity's confidentiality requirements from vendors and other third parties whose products and services compromise part of the system and have access to confidential information.
1.4.1	The organization maintains a non-disclosure agreement signed by third parties prior to sharing information with them.
1.5	Compliance with confidentiality commitments and requirements by vendors and other third parties whose products and services comprise part of the system is assessed on a periodic and as-needed basis and corrective action is taken, if necessary.
1.5.1	The organization monitors third-party service providers' service delivery and compliance status.
1.6	Changes to confidentiality commitments and requirements are communicated to internal and external users, vendors, and other third parties whose products and services are included in the system.
1.6.1	The organization's information security policy is distributed to personnel and business partners.

COMPLEMENTARY USER-ENTITY CONTROLS

Integ's services are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report. Integ's management makes control recommendations to user organizations and provides the means to implement these controls in many instances. Integ also provides best practice guidance to clients regarding control element outside the sphere of Integ responsibility.

This section describes additional controls that should be in operation at user organizations to complement the Integ controls. Client Consideration recommendations include:

- User organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with Integ.
- User organizations should practice removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with Integ's services.
- Transactions for user organizations relating to Integ's services should be appropriately authorized, and transactions should be secure, timely, and complete.
- For user organizations sending data to Integ, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.
- User organizations should implement controls requiring additional approval procedures for critical transactions relating to Integ's services.
- User organizations should report to Integ in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Integ.
- User organizations are responsible for notifying Integ in a timely manner of any changes to personnel directly involved with services performed by Integ. These personnel may be involved in financial, technical or ancillary administrative functions directly associated with services provided by Integ.
- User organizations are responsible for adhering to the terms and conditions stated within their contracts with Integ.
- User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by Integ.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

Privacy Policy

State of Texas
Version Date: July 17, 2017

GENERAL

Anderton Group II LTD (“Company” or “we” or “us” or “our”) respects the privacy of its users (“user” or “you”) that uses our services including other media forms, media channels, mobile website or mobile application related or connected thereto. The following Company privacy policy (“Privacy Policy”) is designed to inform you, as a user of the Website and our services, about the types of information that Company may gather about or collect from you. It also is intended to explain the conditions under which Company uses and discloses that information, and your rights in relation to that information. Changes to this Privacy Policy are discussed at the end of this document. Our Website is hosted in the United States of America and is subject to U.S. state and federal law. If you are accessing our Website from other jurisdictions, please be advised that you are transferring your personal information to us in the United States, and by using our Website, you consent to that transfer and use of your personal information in accordance with this Privacy Policy. You also agree to abide by the applicable laws of applicable states and U.S. federal law concerning your use of the Website and your agreements with us. Any persons accessing our Website from any jurisdiction with laws or regulations governing the use of the Internet, including personal data collection, use and disclosure, different from those of the jurisdictions mentioned above may only use the Website in a manner lawful in their jurisdiction. If your use of the Website would be unlawful in your jurisdiction, please do not use the Website.

BY USING OR ACCESSING THE WEBSITE, YOU ARE ACCEPTING THE PRACTICES DESCRIBED IN THIS PRIVACY POLICY.

GATHERING, USE AND DISCLOSURE OF NON-PERSONALLY-IDENTIFYING INFORMATION

Users of the Website Generally

“Non-Personally-Identifying Information” is information that, without the aid of additional information, cannot be directly associated with a specific person. “Personally-Identifying Information,” by contrast, is information such as a name or email address that, without more, can be directly associated with a specific person. Like most website operators, Company gathers from users of the Website Non-Personally-Identifying Information of the sort that Web browsers, depending on their settings, may make available. That information includes the user’s Internet Protocol (IP) address, operating system, browser type and the locations of the websites the user views right before arriving at, while navigating and immediately after leaving the Website. Although such information is not Personally-Identifying Information, it may be possible for Company to determine from an IP address a user’s Internet service provider and the geographic location of the visitor’s point of connectivity as well as other statistical usage data. Company analyzes Non-Personally-Identifying Information gathered from users of the Website to help Company better understand how the Website is being used. By identifying patterns and trends in usage, Company is able to better design the Website to improve users’ experiences, both in terms of content and ease of use. From time to time, Company may also release the Non-Personally-Identifying Information gathered from Website users in the aggregate, such as by publishing a report on trends in the usage of the Website.

Web Cookies

A “Web Cookie” is a string of information which assigns you a unique identification that a website stores on a user’s computer, and that the user’s browser provides to the website each time the user submits a query to the website. We use cookies on the Website to keep track of services you have used, to record registration information regarding your login name and password, to record your user preferences, to keep you logged into the Website and to facilitate purchase procedures. Company also uses Web Cookies to track the pages that users visit during each Website session, both to help Company improve users’ experiences and to help Company understand how the Website is being used. As with other Non-Personally-Identifying Information gathered from users of the Website, Company analyzes and discloses in aggregated form information gathered using Web Cookies, so as to help Company, its partners and others better understand how the Website is being used. COMPANY USERS WHO DO NOT WISH TO HAVE WEB COOKIES PLACED ON THEIR COMPUTERS SHOULD SET THEIR BROWSERS TO REFUSE WEB COOKIES BEFORE ACCESSING THE WEBSITE, WITH THE UNDERSTANDING THAT CERTAIN FEATURES OF THE WEBSITE MAY NOT FUNCTION PROPERLY WITHOUT THE AID OF WEB COOKIES. WEBSITE USERS WHO REFUSE WEB COOKIES ASSUME ALL RESPONSIBILITY FOR ANY RESULTING LOSS OF FUNCTIONALITY.

Web Beacons

A “Web Beacon” is an object that is embedded in a web page or email that is usually invisible to the user and allows website operators to check whether a user has viewed a particular web page or an email. Company may use Web Beacons on the Website and in emails to count users who have visited particular pages, viewed emails and to deliver co-branded services. Web Beacons are not used to access users’ Personally-Identifying Information. They are a technique Company may use to compile aggregated statistics about Website usage. Web Beacons collect only a limited set of information, including a Web Cookie number, time and date of a page or email view and a description of the page or email on which the Web Beacon resides. You may not decline Web Beacons. However, they can be rendered ineffective by declining all Web Cookies or modifying your browser setting to notify you each time a Web Cookie is tendered, permitting you to accept or decline Web Cookies on an individual basis.

Analytics

We may use third-party vendors, including Google, who use first-party cookies (such as the Google Analytics cookie) and third-party cookies (such as the DoubleClick cookie) together to inform, optimize and serve ads based on your past activity on the Website, including Google Analytics for Display Advertising. The information collected may be used to, among other things, analyze and track data, determine the popularity of certain content and better understand online activity. If you do not want any information to be collected and used by Google Analytics, you can install an opt-out in your web browser (https://tools.google.com/dlpage/gaoptout/) and/or opt out from Google Analytics for

Display Advertising or the Google Display Network by using Google's Ads Settings (www.google.com/settings/ads).

Aggregated and Non-Personally-Identifying Information

We may share aggregated and Non-Personally Identifying Information we collect under any of the above circumstances. We may also share it with third parties and our affiliate companies to develop and deliver targeted advertising on the Website and on websites of third parties. We may combine Non-Personally Identifying Information we collect with additional Non-Personally Identifying Information collected from other sources. We also may share aggregated information with third parties, including advisors, advertisers and investors, for the purpose of conducting general business analysis. For example, we may tell our advertisers the number of visitors to the Website and the most popular features or services accessed. This information does not contain any Personally-Identifying Information and may be used to develop website content and services that we hope you and other users will find of interest and to target content and advertising.

Mobile Device Additional Terms

- Mobile Device. If you use a mobile device to access the Website or download any of our applications, we may collect device information (such as your mobile device ID, model and manufacturer), operating system, version information and IP address.
- Geo-Location Information. Unless we have received your prior consent, we do not access or track any location-based information from your mobile device at any time while downloading or using our mobile application or our services, except that it may be possible for Company to determine from an IP address the geographic location of your point of connectivity, in which case we may gather and use such general location data.
- Push Notifications. We send you push notifications if you choose to receive them, letting you know when someone has sent you a message or for other service-related matters. If you wish to opt-out from receiving these types of communications, you may turn them off in your device's settings.
- Mobile Analytics. We use mobile analytics software to allow us to better understand the functionality of our mobile software on your phone. This software may record information, such as how often you use the application, the events that occur within the application, aggregated usage, performance data and where the application was downloaded from. We do not link the information we store within the analytics software to any Personally-Identifying Information you submit within the mobile application.

COLLECTION, USE AND DISCLOSURE OF PERSONALLY-IDENTIFYING INFORMATION

Website Registration

As defined above, Personally-Identifying Information is information that can be directly associated with a specific person. Company may collect a range of Personally-Identifying Information from and about Website users. Much of the Personally-Identifying Information collected by Company about users is information provided by users themselves when (1) registering for our service, (2) logging in with social network credentials, (3) participating in polls, contests, surveys or other features of our service, or responding to offers or advertisements, (4) communicating with us, (5) creating a public profile or (6) signing up to receive newsletters. That information may include each user’s name, address, email address and telephone number, and, if you transact business with us, financial information such as your payment method (valid credit card number, type, expiration date or other financial information). We also may request information about your interests and activities, your gender, age, date of birth, username, hometown and other demographic or relevant information as determined by Company from time to time. Users of the Website are under no obligation to provide Company with Personally-Identifying Information of any kind, with the caveat that a user’s refusal to do so may prevent the user from using certain Website features.

BY REGISTERING WITH OR USING THE WEBSITE, YOU CONSENT TO THE USE AND DISCLOSURE OF YOUR PERSONALLY-IDENTIFYING INFORMATION AS DESCRIBED IN THIS “COLLECTION, USE AND DISCLOSURE OF PERSONALLY-IDENTIFYING INFORMATION” SECTION.

Company Communications

We may occasionally use your name and email address to send you notifications regarding new services offered by the Website that we think you may find valuable. We may also send you service-related announcements from time to time through the general operation of the service. Generally, you may opt out of such emails at the time of registration or through your account settings, though we reserve the right to send you notices about your account, such as service announcements and administrative messages, even if you opt out of all voluntary email notifications.

Company Disclosures

Company will disclose Personally-Identifying Information under the following circumstances:

- By Law or to Protect Rights. When we believe disclosure is appropriate, we may disclose Personally-Identifying Information in connection with efforts to investigate, prevent or take other action regarding illegal activity, suspected fraud or other wrongdoing; to protect and defend the rights, property or safety of Company, our users, our employees or others; to comply with applicable law or cooperate with law enforcement; to enforce our Terms of Use or other agreements or policies, in response to a subpoena or similar investigative demand, a court order or a request for cooperation from a law enforcement or other government agency; to establish or exercise our legal rights; to defend against legal claims; or as otherwise required by law. In such cases, we may raise or waive any legal objection or right available to us.
- Marketing Communications. Unless users opt-out from receiving Company marketing materials upon registration, Company may email users about products and services that Company believes may be of interest to them. If you wish to opt-out of receiving marketing materials from Company, you may do so by following the unsubscribe link in the email communications, by going to your account settings (if applicable) or contacting us using the contact information below.
- Third-Party Service Providers. We may share your Personally-Identifying Information, which may include your name and contact information (including email address) with our authorized service providers that perform certain services on our behalf. These services may include fulfilling orders, providing customer service and marketing assistance, performing business and sales analysis, supporting the Website’s

functionality and supporting contests, sweepstakes, surveys and other features offered through the Website. We may also share your name, contact information and credit card information with our authorized service providers who process credit card payments. These service providers may have access to personal information needed to perform their functions but are not permitted to share or use such information for any other purpose.

- Business Transfers; Bankruptcy. Company reserves the right to transfer all Personally-Identifying Information in its possession to a successor organization in the event of a merger, acquisition, bankruptcy or other sale of all or a portion of Company's assets. Other than to the extent ordered by a bankruptcy or other court, the use and disclosure of all transferred Personally-Identifying Information will be subject to this Privacy Policy, or to a new privacy policy if you are given notice of that new privacy policy and are given an opportunity to affirmatively opt-out of it. Personally-Identifying Information submitted or collected after a transfer, however, may be subject to a new privacy policy adopted by the successor organization.

Changing Personally-Identifying Information; Account Termination

You may at any time review or change your Personally-Identifying Information by going to your account settings (if applicable) or contacting us using the contact information below. Upon your request, we will deactivate or delete your account and contact information from our active databases. Such information will be deactivated or deleted as soon as practicable based on your account activity and accordance with our deactivation policy and applicable law. To make this request, either go to your account settings (if applicable) or contact us as provided below. We will retain in our files some Personally-Identifying Information to prevent fraud, to troubleshoot problems, to assist with any investigations, to enforce our Terms of Use and to comply with legal requirements as is permitted by law. Therefore, you should not expect that all your Personally-Identifying Information will be completely removed from our databases in response to your requests. Additionally, we keep a history of changed information to investigate suspected fraud with your account.

General Use

Company uses the Personally-Identifying Information in the file we maintain about you, and other information we obtain from your current and past activities on the Website (1) to deliver the products and services that you have requested; (2) to manage your account and provide you with customer support; (3) to communicate with you by email, postal mail, telephone and/or mobile devices about products or services that may be of interest to you either from us, our affiliate companies or other third parties; (4) to develop and display content and advertising tailored to your interests on the Website and other sites; (5) to resolve disputes and troubleshoot problems; (6) to measure consumer interest in our services; (7) to inform you of updates; (8) to customize your experience; (9) to detect and protect us against error, fraud and other criminal activity; (10) to enforce our Terms of Use; and (11) to do as otherwise described to you at the time of collection. At times, we may look across multiple users to identify problems. In particular, we may examine your Personally-Identifying Information to identify users using multiple user IDs or aliases. We may compare and review your Personally-

Identifying Information for accuracy and to detect errors and omissions. We may use financial information or payment method to process payment for any purchases made on the Website, enroll you in the discount, rebate, and other programs in which you elect to participate, to protect against or identify possible fraudulent transactions and otherwise as needed to manage our business.

COLLECTION AND USE OF INFORMATION BY THIRD PARTIES GENERALLY

Company contractually prohibits its contractors, affiliates, vendors and suppliers from disclosing Personally-Identifying Information received from Company, other than in accordance with this Privacy Policy. However, third parties are under no obligation to comply with this Privacy Policy with respect to Personally-Identifying Information that users provide directly to those third parties, or that those third parties collect for themselves. These third parties include advertisers, providers of games, utilities, widgets and a variety of other third-party applications accessible through the Website. Company neither owns nor controls the third-party websites and applications accessible through the Website. Thus, this Privacy Policy does not apply to information provided to or gathered by the third parties that operate them. Before visiting a third party, or using a third-party application, whether by means of a link on the Website, directly through the Website or otherwise, and before providing any Personally-Identifying Information to any such third party, users should inform themselves of the privacy policies and practices (if any) of the third party responsible for that website or application, and should take those steps necessary to, in those users' discretion, protect their privacy.

SECURITY

We take the security of your Personally-Identifying Information seriously and use reasonable electronic, personnel and physical measures to protect it from loss, theft, alteration or misuse. However, please be advised that even the best security measures cannot fully eliminate all risks. We cannot guarantee that only authorized persons will view your information. We are not responsible for third-party circumvention of any privacy settings or security measures.

We are dedicated to protect all information on the Website as is necessary. However, you are responsible for maintaining the confidentiality of your Personally-Identifying Information by keeping your password confidential. You should change your password immediately if you believe someone has gained unauthorized access to it or your account. If you lose control of your account, you should notify us immediately.

PRIVACY POLICY CHANGES

Company may, in its sole discretion, change this Privacy Policy from time to time. Any and all changes to Company's Privacy Policy will be reflected on this page and the date new versions are posted will be stated at the top of this Privacy Policy. Unless stated otherwise, our current Privacy Policy applies to all information that we have about you and your account. Users should regularly check this page for any changes to this Privacy Policy. Company will always post new versions of the Privacy Policy on the Website. However, Company may, as determined in its discretion, decide to notify users of changes made to this Privacy Policy via email or otherwise. Accordingly, it is important that users always maintain and update their contact information.

CHILDREN

The Children's Online Privacy Protection Act ("COPPA") protects the online privacy of children under 13 years of age. We do not knowingly collect or maintain Personally-Identifying Information from anyone under the age of 13, unless or except as permitted by law. Any person who provides Personally-Identifying Information through the Website represents to us that he or she is 13 years of age or older. If we learn that Personally-Identifying Information has been collected from a user under 13 years of age on or through the Website, then we will take the appropriate steps to cause this information to be deleted. If you are the parent or legal guardian of a child under 13 who has become a member of the Website or has otherwise transferred Personally-Identifying Information to the Website, please contact Company using our contact information below to have that child's account terminated and information deleted.

CALIFORNIA PRIVACY RIGHTS

California Civil Code Section 1798.83, also known as the "Shine The Light" law, permits our users who are California residents to request and obtain from us, once a year and free of charge, information about the Personally-Identifying Information (if any) we disclosed to third parties for direct marketing purposes in the preceding calendar year. If applicable, this information would include a list of the categories of the Personally-Identifying Information that was shared and the names and addresses of all third parties with which we shared Personally-Identifying Information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to our privacy officer as listed below.

DO-NOT-TRACK POLICY

Most web browsers and some mobile operating systems include a Do-Not-Track (“DNT”) feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. Because there is not yet a common understanding of how to interpret the DNT signal, the Website currently does not respond to DNT browser signals or mechanisms.

CONTACT

If you have any questions regarding our Privacy Policy, please contact our Privacy Officer at:

Anderton Group II LTD
Attn: Privacy Officer
700 W. Loop 340
Waco, TX 76712
Email: info@integdoes.com
Phone: (254) 751-1012

integ
DATA | PRINT | MAIL

Anderton Group, Inc. (AGI) / Anderton Group II, LTD (AGL)
700 W. Loop 340
Waco, TX 76712-6866

The Anderton Group II, LTD Family of Integ Companies Includes:

Gatesville Printing & Office Supply
Postal Methods

Proprietary Information and Non-Disclosure Agreement

In partial consideration of continual employment, employee acknowledges that/and agrees to:

During employment, the Employee will have access to and become familiar with various trade secrets, consisting of customer's prices and requirements, secret inventions, processes, and compilations of information, records and specifications, owned by the Employer (AGI/AGL) and regularly used in the operation of the business of the Employer. The Employee shall not disclose any such information. All files, records, documents, software, drawings, specifications, equipment, and similar items relating to the business of the employer, whether or not prepared by the Employee, shall remain the exclusive property of the Employer and shall not be removed from the premises of the Employer under any circumstances without prior written consent of the Employer.

Employee shall maintain all confidential and proprietary information disclosed or received by Employee in confidence unless AGI/AGL specifically authorizes otherwise in writing. Employee shall not copy confidential and proprietary information, in whole or in part, without the prior written consent of AGI/AGL. Employee shall return the original and any and all copies of confidential and proprietary information to AGI/AGL promptly upon written request. Employee shall not divulge or disclose to any third party, in whole or in part, confidential and proprietary information. This obligation continues after the Employee terminates, whether voluntarily or involuntarily.

The Employer/Employee have executed this agreement on the _______day of_________ 2_____

______________________________	______________________________
Employee Signature	AGI/AGL Representative