affinity

REPORT ON CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

SOC 3

NOVEMBER 1, 2019 TO OCTOBER 31, 2020

linford&co llp
cpa firm

linford&co llp
cpa firm

▪ linford&co llp
1550 wewatta st, 2nd floor
denver, co 80202

▪ tel: +1 (720) 330 7201
email: info@linfordco.com
www.linfordco.com

Section I – Independent Service Auditor's Report

To the Board of Directors of Project Affinity, Inc.:

Scope

We have examined Project Affinity, Inc.'s (Affinity or the Company) accompanying assertion titled "Assertion of Project Affinity's Management" (assertion) that the controls within Affinity's relationship intelligence services (system) were effective throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that Affinity's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Affinity is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Affinity's service commitments and system requirements were achieved. Affinity has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Affinity is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted 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 management's assertion is fairly stated in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- ✓ Obtaining an understanding of the system and service organization's service commitments and system requirements.
- ✓ Assessing the risks that controls were not effective to achieve Affinity's service commitments and system requirements based on the applicable trust services criteria.
- ✓ Performing procedures to obtain evidence about whether controls within the system were effective to achieve Affinity's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Affinity's relationship intelligence services were effective throughout the period November 1, 2019 to October 31, 2020 to provide reasonable assurance that Affinity's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

linford&co llp

December 10, 2020
Denver, Colorado

Section II –Assertion of Project Affinity's Management

December 10, 2020

We are responsible for designing, implementing, operating, and maintaining effective controls within Project Affinity, Inc.'s (Affinity or the company) relationship intelligence services throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that Affinity's services commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

We have prepared an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2019 to October 31, 2020 to provide reasonable assurance that Affinity's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Affinity's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that Affinity's service commitments and system requirements were achieved based on the applicable trust services criteria.

Adam Perelman
Chief Technology Officer

Section III – Project Affinity's Description of Its Relationship Intelligence Services

Overview of Operations

Project Affinity, Inc. develops network and customer relationship management solutions for enterprises. Its solutions feature relationship management, email detection, network search, network intelligence, automatic data capture, collaboration and reminders, and a browser extension. The company was founded in 2014 and is based in San Francisco, California.

Principal Service Commitments and System Requirements

Affinity designs its processes and procedures to meet objectives for its relationship intelligence services. Those objectives are based on the service commitments that Affinity makes to user entities and the compliance requirements that Affinity has established for their services.

Security commitments to user entities are documented and communicated in their customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the relationship intelligence services are implemented to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Controlled access to the production environment and the supporting infrastructure.
- Segregation of client data.
- Monitoring of system performance metrics and critical application services.

Affinity establishes operational requirements that support the achievement of security, availability, and confidentiality commitments and other system requirements. Such requirements are communicated in Affinity system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal networks are managed, and how employees are hired and trained.

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, Monitoring, and Control Activities for the Security, Availability, and Confidentiality Criteria

A company's entity-level controls reflect the overall attitude, awareness, and actions of management and others concerning the importance of controls and the emphasis given to controls in the company's policies, procedures, methods, and organizational structure. Entity-level controls are not specific to any individual transaction, but applies to the company as a whole. These types of controls are necessary to facilitate the proper functioning of activity level controls supporting the relationship intelligence services. Throughout this section, a description of the five components of internal control (control environment, risk assessment, information and communication, monitoring, and control activities) as they relate to the services Affinity provides to its clients.

The controls supporting the control objectives identified by Affinity were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Control objectives and controls designed, implemented, and operated to meet them, ascertain that the system is protected against unauthorized access (both physical and logical). Entity-level controls and specific control activities supporting the applicable trust services criteria are provided in the descriptions of this section of the report.

Control Environment

A board of directors exercises independent oversight of Affinity's strategic direction, operational performance, and internal control. Affinity's board of directors is made up of internal executives as well as external leadership. The board of directors sets the tone at the top of the organization that is followed by all employees. The tone is demonstrated through their directives, actions, and behavior and highlights the importance of integrity and ethical values to support the functioning of the system of internal control. The board of directors meets on a quarterly basis. To help determine expectations are understood by employees, executive management has established a code of conduct. The primary goal of Affinity's code of conduct is to foster inclusive, collaborative, and safe working conditions for all Affinity staff.

Affinity is committed to providing a friendly, safe, and welcoming environment for all staff, regardless of gender, sexual orientation, ability, ethnicity, socioeconomic status, and religion. The documented code of conduct applies to all Affinity full-time, part-time, and contractor staff and includes the following sections: culture and citizenship, accepted and expected behavior, unacceptable behavior, weapons policy, sanctions for non-compliance, and reporting violations.

Continuous Independent Compliance and Security Monitoring: Affinity uses a tool called Vanta which objectively and continuously monitors the Affinity control environment and alerts management when many types of internal control and security issues arise.

Organizational Structure: Management has established structures, reporting lines, and appropriate authorities in the pursuit of Affinity's business objectives. The structures, reporting lines, and authority are clearly communicated through management's operational style, the organizational structure, policies and procedures, and employee job descriptions. Affinity's organizational structure is organized into several departments including: Engineering, Sales and Marketing, and Operations. The role of Security Officer has been assigned and communicated throughout the organization. The Security Officer is responsible for the security of Affinity's systems.

Hiring: When a position is open at Affinity, a job description and listing will be posted on Affinity's website, as well as on other job forums. Additionally, Affinity sources candidates via referrals, cold reach-outs to candidates, external recruiting agencies, and campus recruiting. Resumes of applicants are received and reviewed by the hiring manager. The interview process is tailored to match the position being hired for. If the role is technical, there will be technical interviews of the candidates, or if the role is for sales, a mock sales demo will be required. Interviews generally start as phone interviews, with the final interview being onsite (this is sometimes a "virtual" onsite if an office visit is impractical). Following each interview, the interviewer will submit written feedback about a candidate in the applicant tracking system. Reference checks are performed after the final interview before a final decision on the candidate is made. Following the in-person interview and the reference checks, candidates with most or all of the desired attributes are extended an offer for employment. Once an applicant is selected internally, an offer letter is sent to the selected applicant, which states that the applicant will be hired pending a successful background check. Applicants for full-time Affinity employment that may have access to client data are required to complete a successful background check, which includes a social security verification, education and employment history verification, federal and state criminal check, government sections, and sex offender database check.

New Hires: Onboarding consists of completing the employment documentation and reviewing and acknowledging all policies and procedures, as well as training. New hires are required to complete Affinity security awareness training before assuming their position.

Performance and Feedback: Affinity evaluates competence across the entity in relation to established policies and practices and acts as necessary to address shortcomings. Affinity has documented a policy for evaluating employee performance and feedback. Affinity believes feedback is forward-looking and is information that someone can use to grow and develop. Performance assessments, however, look to the past to discover how an individual performed over the last six months. Feedback is provided on an ongoing and bi-annual basis.

Employment-at-Will: All new hires sign an employment agreement with the Company that includes "at-will" employment language. As part of the terms of the employment agreement with individuals, Affinity maintains the right to discipline or terminate individuals based on a pattern of poor job performance. Additionally, under at-will employment law, employees can be terminated at any time for any reason.

Communication and Information

Internal Control Monitoring: Affinity obtains or generates and uses relevant, quality information to support the functioning of internal control. Affinity uses a variety of methods to monitor production systems and internal controls. The methods include the Vanta tool for monitoring internal controls relevant to SOC 2 compliance, as well as application and infrastructure monitoring tools and penetration testing.

Internal Communication: Affinity maintains security policies to communicate security responsibilities to Affinity personnel. The policies include objectives and responsibilities for internal control necessary to support the functioning of internal control. Policies are reviewed at least annually and updated as necessary. In addition to policies and procedures, Affinity uses an internal communication tool that is used for collaboration and communication including responsibilities related to security. The communication tool is used by entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls to communicate about responsibilities, including changes in responsibilities.

Annual Security Awareness Training: To assist with Affinity's commitments to security, Affinity management provides annual security awareness training for all employees that covers information security, data protection, and confidentiality of client information.

External Communication: Affinity has also created a high-level overview of the Affinity system used to describe the services provided to the clients that Affinity serves. Affinity and its clients' responsibilities and commitments regarding the acceptable use of the Affinity system are included within the Affinity Master Services Agreement (MSA), which clients must agree to before using the Affinity system. The Affinity site https://status.affinity.co/ communicates changes and status to the application and the impact on users.

Incident Reporting: Affinity has provided information to clients and employees on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by Affinity in the event there are problems. Clients may contact Affinity support via the Affinity support site at https://support.affinity.co. Affinity personnel may contact their supervisor to report important matters requiring attention.

Risk Assessment

Affinity Risk Assessment and Management Program: Affinity's Risk Assessment and Management Program policy describes the processes Affinity has in place to identify new business and technical risks and how frequently those risks are mitigated. The policy designates responsibility for risk management at Affinity and outlines the process for identifying and addressing risks to the confidentiality, integrity, and availability of client data that Affinity accesses, stores, and transmits. The policy is made available to all employees through the Company's Vanta tool.

Principles: Affinity specifies risk management objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. Affinity is proactive in its approach to risk management, balancing the cost of managing risk with anticipated benefits, and undertaking contingency planning in the event that critical risks are realized. Affinity's primary duty is to ascertain that the security, availability, and confidentiality of critical systems and customer data. The duty to maintain a secure and available infrastructure requires Affinity to identify and manage risks.

Affinity believes that effective risk management involves:

1. A commitment to the security, availability, and confidentiality of Affinity infrastructure and services from senior management;
2. The involvement, cooperation, and insight of all Affinity staff;
3. A commitment to initiating risk assessments, starting with discovery and identification of risks;
4. A commitment to the thorough analysis of identified risks;
5. A commitment to the strategy and treatment of identified risks;
6. A commitment to communicate all identified risks to the company;
7. A commitment to encourage the reporting of risks and threat vectors from all Affinity staff.

Affinity believes that the following events should trigger a risk assessment to occur:

1. A significant and major change to existing infrastructure, product, or business practices;
2. A significant amount of time (a year) has passed since the last risk assessment.

Scope: The Risk Assessment and Management program applies to all systems and data on the Affinity network, owned by Affinity or its customers, or operated on behalf of the organization. Affinity risk assessments evaluate infrastructure such as computer infrastructure containing networks, instances, databases, systems, storage, and services. Affinity risk assessments also include an analysis of business practices, procedures, and physical office spaces as needed.

Risk assessments may be high level or detailed to a specific organizational or technical change as Affinity stakeholders and technologists see fit. Risk assessments must be conducted by unbiased and qualified parties such as security consultancies or qualified internal staff.

Risk Management Oversight: Overall, the execution, development, and implementation of risk assessments and remediation programs is the joint responsibility of Affinity's CTO and the department or individuals responsible for the area being assessed. All staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff are further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Commitments

- Affinity performs at least one risk assessment annually using qualified internal staff and/or external third parties who have experience performing risk assessments.
- A risk assessment should be performed or reviewed on critical systems and applications no less than every two years.

- Risk assessments should be used to assess all risks to the organization.
- All staff involved in a risk assessment must fully cooperate with the risk assessment project lead conducting the assessment and developing a remediation strategy.
- Any staff members or external consultants who perform Affinity risk assessments are required to be familiar with computer technology and computer security in use by Affinity. The risk assessment project leader should be the security officer or a staff member the security officer designates to conduct the risk assessment.
- Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks. The action plan may be included with the risk assessment report, or separately. The action plan will be an action plan for implementing additional controls and solutions to mitigate or manage the risk. The action plan may define participants and actions to be taken during the implementation of the action plan.
- The risk assessment process and methodology will be updated as required due to results of audits and incidents.
- All identified vulnerabilities are assessed for impact and criticality. Vulnerabilities must be remediated as soon as possible as mandated by the Affinity Vulnerability and Patch Management Program.

Risk Assessment Process: Affinity's risk assessment methodology is based off *NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments*. Management defines the scope of the risk assessment and creates the risk assessment team with a point person to guide the process (risk assessment project lead). If risk assessment procedures are not defined, the team must define them. The proper time and method of communicating the selected risk treatment options to the affected IT and business management should be included.

- Determine if the system is critical to the organization's business processes and determine the data classification and security needs of the data on the system according to the Affinity Data Classification Policy, considering security, availability, and confidentiality needs.
- List possible threat sources such as an exploitation of a vulnerability.
- Identify vulnerabilities.
- Evaluate potential security controls already in place to assess if they adequately address the risk.
- Identify probability of exploitation. Additional security controls may need to be in place before the probability of exploitation is lowered.
- Categorize the damage (impact) and possibly place a dollar amount on the damage where possible.
- Use (likelihood * impact) to quantify the amount of risk.
- List specific vulnerabilities and threats to the system and identify mitigating controls.
- Identify existing controls and those that may further mitigate specific vulnerabilities.
- Create the risk assessment report.
- Communicate the selected risk treatment options to the affected IT and business management staff.
- Take recommended risk mitigation actions. Record such actions as changes per the Affinity Change Management program.
- Monitor the effectiveness of risk mitigation actions and document the results.

Vendor Risk Management: Affinity relies on vendors to perform a variety of services, some of which are critical for operations. Affinity aims to manage its relationship with vendors and minimize the risk associated with engaging third parties to perform services. The Vendor Risk Management policy provides a framework for managing the lifecycle of vendor relationships. Risk assessments for vendors are covered under Affinity's Vendor Management Program, which includes a thorough risk assessment targeted at a particular vendor's security, business practices, and legal commitments.

Fraud Risk: Affinity has considered the potential for fraud when assessing risks to the achievement of objectives. There is a low risk of fraud since the Affinity application is used for collaboration purposes only and does not allow the transfer of money.

Change Identification and Risk Assessment: Affinity's risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.

Logging and Monitoring

Application Logging and Monitoring: Affinity uses monitoring tools to monitor application health and these monitoring tools alerts system administrators when the application in not operating within defined boundaries. Affinity uses various third-party tools for monitoring, as well as internally developed monitoring tools. When alerts from the tools are received, they are followed up on until they are resolved.

Infrastructure Logging and Monitoring: Affinity also logs authentication, availability, and error events and uses tools for infrastructure monitoring. Every authentication event to the application and infrastructure records a log event that may be used later for forensic purposes to research security incidents.

Affinity Vulnerability Management and Patch Program: Affinity's Vulnerability Management policies and procedures describe what is in place to monitor for new vulnerabilities, how often vulnerabilities are addressed, and the way in which those new vulnerabilities are addressed.

On average, 20 to 30 new vulnerabilities are released into the wild every day. Affinity's internal vulnerability monitoring and external vulnerability scanning are in place to keep up with new threats while validating security controls put in place so that Affinity's security posture is maintained.

Vulnerability Management and Patch Policy:

- Affinity performs internal vulnerability scanning and package monitoring on a continuous basis using:
    - Vulnerability alerts on GitHub
    - AWS Inspector
    - HackerOne bug bounty program
    - Third-party penetration testing firms
    - Vanta Continuous Security and Compliance Monitoring
- Affinity performs external vulnerability scanning daily using Tenable. External web endpoints, company APIs, etc. are subject to external vulnerability scanning.

- Security team members are responsible for communicating detected vulnerabilities and package updates needed to the appropriate engineering staff for resolution. Engineering staff are responsible for various infrastructure components and are responsible for resolving detected vulnerabilities in a timely manner as defined by Affinity's timing standards.

Severity and Timing: Affinity defines the severity of an issue via industry-recognized Common Vulnerability Scoring System (CVSS) scores, which all modern scanning and continuous monitoring mechanisms utilize. The CVSS provides a way to capture the characteristics of a vulnerability, and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Vulnerability and Patch Management Process Flow:

1. A new vulnerability or a new patch is detected from the various monitoring and scanning Affinity has in place.
2. The security team enters vulnerability or patch details and instructions into Affinity's change management system, which is Asana, and assigns the ticket to the appropriate team member to address.
3. The ticket assignee follows the change management process to implement the necessary change to apply the patch or address the new vulnerability.
4. The ticket is updated with results from the applied change, detailing any exceptions into the Affinity risk register.
5. The security team checks the source from which the vulnerability originated to determine that the change performed has addressed the vulnerability detected. The ticket is updated with the results and closed out.

Responsible Disclosure Program: In addition to monitoring for vulnerabilities using scans and tools, Affinity has implemented a responsible disclosure program for users to report issues and vulnerabilities associated with their use of the Affinity application.

Penetration Testing: Affinity annually has a third-party application penetration test performed. Issues identified during the tests are remediated as necessary.

Control Activities

Affinity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. Control activities include a variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls as well as preventive and detective controls. Management has established and implemented policies and procedures to help determine periodic assessments and evaluations are performed that consider all elements of security as it applies to

the AICPA Trust Services Criteria. The policies include control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats. Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary. In addition, management takes corrective action when issues are identified with control activities.

Logical and Physical Access

Affinity System Access and Authorization Control Policy: Each Affinity employee, contractor, and associate has limited access to Affinity systems and applications. Access is always provisioned on a minimum-necessary (least-privilege) basis. Affinity's System Access and Authorization Control Policy documents the requirements for registering and authorizing employees prior to being issued system credentials and granted the ability to access the system.

Employee Access to Affinity Systems: Access to Affinity systems and third-party accounts owned by Affinity are only granted on a need-to-use basis, as defined by the responsibilities of the position held and the duties of the position. Access control and management is divided into multiple phases of the account lifecycle which include: creation, privilege management, authorization, password management, audit, and revocation.

Authorization - Role Based Access Control:

- In most cases, Affinity employees are granted access to Affinity systems according to their role and/or team.
- The executive team and team managers are jointly responsible for maintaining a list of roles and associated access scope for team members.
- If an Affinity employee requires access outside of the standard for their role or team, either they or their managers may initiate an access request, following the policy outlined in "Access Requests," as follows.

Creation - Access Requests:

- Access requests for Affinity employees are made by employees and their managers.
- Access requests should be made to the Affinity employee or employees who manage the relevant resource(s).
- Those employees will not grant access unless they are satisfied the additional access is necessary for the grantee to complete a necessary business task.

In addition, the employee(s) must accept the company's Acceptable Use Policy before access will be granted.

- When granting access, employees will scope grants to the minimum duration to complete the relevant business task. Root access is not granted unless absolutely necessary to perform the job function.

Privilege Management

- Affinity's CTO will determine and maintain appropriate assignment of privilege within Affinity's production, development, and test applications and environments.
- Affinity's CTO will determine and maintain appropriate assignment of privilege within Affinity's databases.
- Affinity's CTO will determine and maintain appropriate assignment within supporting infrastructure.

Account Audit: The responsible team will conduct quarterly audits of accounts, privileges, and password management, and is required to document access change requests in Asana.

Revocation: Role Changes and Termination

- Managers must notify the company's CTO if an employee has been terminated or changes roles.
- In the case of termination, the former employee's access is required to be revoked within three days.
- In the case of a role change, the employee's access should be revised within three days after changing roles.
- In some cases, access will be revoked as a disciplinary measure for policy violation.

Administrator and Remote Access: Administrator-level access privileges to the production environment are restricted to only those individuals who require such access to perform their respective job functions. Access is limited to certain individuals who require the ability to add, delete, and modify users' access to the production system. Remote access to the production infrastructure is limited to authorized individuals and communications are encrypted via the use of secure shell (SSH) and AWS console.

Access to Client Data: Client data is stored within Affinity's production database instance. Access to client data within the Affinity production database by Affinity employees is restricted to authorized users. In addition, client users have access to their data only and no other clients' data.

Encryption of Client Data: Affinity understands the sensitivity of its clients' data and has therefore implemented security controls to protect the confidentiality of the data. Client data within Affinity's production databases is encrypted.

Infrastructure Authentication: Multifactor authentication is required for administrator access to the AWS infrastructure.

Workstation Use and Security: The Company's policies and procedures provide guidance to its personnel concerning the physical safeguarding of workstations with access to the IT environment. The guidance is appropriate to the workstation type (e.g., fixed workstation, portable workstation/laptop computer, tablet computer, smartphone, etc.) and location (e.g., office, home, public place, etc.).

Session Lock: Employee workstations are required to be configured to automatically log off after a modest period of inactivity.

Physical Access: Affinity has one physical office located in San Francisco, California. Their office is in a shared office space with an individual locked office that is control by card key. Only authorized individuals (e.g., employees and building management) are allowed to access the Affinity office suite. When an employee terminates employment, their key fob to the Affinity office suite is collected.

Inventory of Information Assets: Affinity maintains an inventory listing of servers and workstations in order to protect them from security events, maintain the confidentiality of data, and ascertain availability. The inventory is dynamically built and constantly updated by the Vanta tool which looks to AWS to see which virtual machines are running. Vanta also prompts management to classify and document information related to each machine.

AWS Bastion Host: A bastion host is used to access the Affinity network. The bastion host VPC rules are configured to block unauthorized traffic into the network. Access to modify VPC rules is restricted to authorized individuals.

Laptop Encryption: To minimize the risk of data being compromised in the event that hardware or data is lost or stolen, Affinity has encrypted all laptops using FileVault for Mac laptops and BitLocker for Windows laptops.

Transmission Encryption: Whether web-based or via mobile applications, all data transfers between users and the Affinity system are secured using Transport Layer Security (TLS) and industry standard encryption. Affinity has also documented a cryptography policy that outlines the requirements for encrypting data and transmissions.

Removable Media: Affinity has taken measures to restrict employee use of removable media to help mitigate both the risk of data loss as well as the risk of malware being introduced onto Affinity systems. By policy, the use of removable media is not allowed.

Hardware and Data Disposal: Affinity's policies related to data protection address the handling of devices and media that may potentially contain sensitive Company or client data, including personally identifiable information (PII). Affinity defines specific requirements for hardware and data disposal in its security policies. Client data is retained indefinitely until the client terminates service. When clients terminate, their data is deleted within one week.

System Operations Controls

Incident Response Program: Affinity has a documented Incident Response Plan (IRP) which establishes the procedures to be undertaken in response to information security incidents. The IRP has been communicated to appropriate personnel and includes the following:

- Escalation procedures
- Incident severity identification and classification
- Roles, responsibilities, and communication strategies in the event of a compromise, to include designation of an Incident Response Team
- Containment and eradication strategies
- Communications protocols, internally and externally
- A retrospective analysis to determine the root cause and implement incident response enhancements

The IRP is updated annually, and more frequently based upon incident outcomes and lessons learned, as appropriate. Affinity responds to and tracks all incidents that occur to resolution per the documented Incident Response Plan (IRP). Incidences that occur also have a post-mortem with lessons learned documented. Gaps, areas of improvement, and lessons learned are utilized to modify the plan, as needed.

Incident Monitoring and Recordkeeping: Affinity maintains a record of security incidents to ascertain the incident was followed through to resolution. The incident records include a description of the incident and relevant facts (e.g., information that was disclosed), mitigations, risk assessment, and outcomes.

Antivirus and Patching: Affinity deploys malware detection software on all workstations that can access the production environment and has configured malware detection software to perform daily scans with immediate notification if malware is detected. Affinity applies security patches to user workstations regularly, so at any given time workstations are on the most current or previous two most current operating system versions. Production servers are monitored continuously within AWS and patches are applied for known vulnerabilities.

Backups: Affinity has documented a backup policy that describes how often service and client data is backed up. All original customer data on Affinity's infrastructure must be backed up. Full database backups are performed daily and automatically by AWS' automated backup service.

Business Continuity Plan: The success of the organization is reliant upon the preservation of critical business operations and essential functions used to deliver key products and services. Affinity has created a business continuity plan to define the criteria for continuing business operations for the organization in the event of a disruption. Specifically, the Business Continuity Plan identifies key resources and needs to ascertain that business may continue, even in a limited capacity, in the event of a disaster. The plan includes information such as key suppliers, contingency plans and alternative business location.

Disaster Recovery Policy: Affinity has created a Disaster Recovery Policy to define the organization's procedures to recover information technology (IT) infrastructure and IT services within set deadlines in the case of a disaster or other disruptive incident. The objective of the policy and procedures is to complete the recovery of IT infrastructure and IT services within a set Recovery Time Objective (RTO). Affinity's RTO is 24 hours. Relocation and restoration of critical services and technologies must be completed within 24 hours.

The following objectives have been established for the policy:

1. Identify the activities, resources, and procedures needed to carry out Affinity processing requirements during prolonged interruptions to normal operations.
2. Identify and define the impact of interruptions to Affinity systems.
3. Assign responsibilities to designated personnel and provide guidance for recovering Affinity during prolonged periods of interruption to normal operations.
4. Ascertain coordination with other Affinity staff who will participate in the contingency planning strategies.
5. Ascertain coordination with external points of contact and vendors who will participate in the contingency planning strategies.

Examples of the types of disasters that would initiate the plan are natural disaster, political disturbances, man-made disasters, external human threats, and internal malicious activities.

Affinity defined two categories of systems from a disaster recovery perspective.

1. Critical Systems. These systems host application servers and database servers or are required for functioning of systems that host application servers and database servers. These systems, if unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable.
2. Non-critical Systems. These are all systems not considered critical by definition above. These systems, while they may affect the performance and overall security of critical systems, do not prevent Critical systems from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems.

Lines of Succession and Responsibilities: Within the disaster recovery plan, there is a notification list. Additionally, responsibilities are documented in the policy. Changes are made as needed to keep the contacts up-to-date.

Testing and Maintenance: The CTO establishes criteria for validation/testing of a Contingency Plan, an annual test schedule, and notes that a test occurs. At a minimum, the Contingency Plan is tested annually (within 365 days). The types of validation/testing exercises include tabletop and technical testing. Contingency Plans for all application systems must be tested at a minimum using the tabletop testing process. However, if the application system Contingency Plan is included in the technical testing of their respective support systems that technical test will satisfy the annual requirement.

Change Management

An effective system development and maintenance process is critical to the availability and integrity of Affinity's system. Affinity is a proprietary and in-house developed system where custom changes are often necessary to enhance system functionality. Affinity follows a defined development policy for making changes to the system used to support the services provided to their clients. Affinity's Change Management

Policy describes how changes to the Affinity system are proposed, reviewed, deployed, and managed. The policy covers all changes made to the Affinity software, regardless of their size, scope, or potential impact.

The policy is designed to mitigate the risks of:

- Corrupted or destroyed information
- Degraded or disrupted computer performance
- Productivity loss
- Introduction of new vulnerabilities, configuration errors, and software bugs in infrastructure and code
- Exposure to reputational risk

A request for a change can come internally from management or externally from a client. A project management tool is used to track which changes are authorized for development. Once assigned, an engineer develops the change and then oversees any needed testing or peer reviews. Engineering uses a software development platform to manage and record activities related to the change management process. The tool enforces version control and is used to document control points within the change management process.

Once a change is ready for deployment to production, the assigned engineer submits the change's pull request for review, testing, and approval to release the change to production. Once approved in the pull request, an engineering manager releases the change to production. Affinity also communicates with stakeholders the progress of changes, product highlights, and current issues on their blog at: https://affinity.co/blog.

Authorization to Implement Changes: Affinity restricts the ability to implement changes into the production environment to only those individuals who require the ability to implement changes as part of their job function.