System and Organization Controls (SOC) 3 Report

Management's Report of Its Assertions on Applied Systems, Inc.'s Applied Cloud System Based on the Trust Services Criteria for Security, Availability and Confidentiality

For the Period November 1, 2019 to October 31, 2020

TABLE OF CONTENTS

SECTION ONE: REPORT OF INDEPENDENT ACCOUNTANTS

To: Management of Applied Systems, Inc.

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of Its Assertions on the Effectiveness of Its Controls over Applied Systems, Inc.'s Applied Cloud System Based on the Trust Services Criteria" (Assertion) that Applied Systems, Inc.'s controls over the Applied Cloud System (System) were effective throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The Assertion also indicates that Applied Systems, Inc.'s ("Service Organization" or "Applied") controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Applied's infrastructure's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Applied uses various subservice organizations to supplement their services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Applied, to achieve Applied's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitably designed or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Applied management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Applied Cloud System and describing the boundaries of the System;
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of the System; and
- Identifying, designing, implementing, operating, and monitoring effective controls over the Applied Cloud System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes:

- Obtaining an understanding of Applied's Applied Cloud System relevant security, availability, and confidentiality policies, procedures, and controls;
- Testing and evaluating the operating effectiveness of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Applied's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent Limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design and operating effectiveness of the controls to achieve Applied's Applied Cloud System's principal service commitments and system requirements, is subject to the risk that controls may become

inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system of controls, may alter the validity of such evaluations.

Opinion

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

CyberGuard Compliance, LLP

November 24, 2020
Orange, California

SECTION TWO: MANAGEMENT'S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER APPLIED SYSTEMS, INC.'S APPLIED CLOUD SYSTEM BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY, AVAILABILITY AND CONFIDENTIALITY

November 24, 2020

Scope

We, as management of Applied Systems, Inc., are responsible for:

- Identifying the Applied Systems, Inc. Applied Cloud System (System) and describing the boundaries of the System, which are presented in the section below (Attachment A) titled Applied Systems, Inc.'s Applied Cloud System (Description);
- Identifying our principal service commitments and system requirements (Attachment B);
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in the section below (Attachment A) Description of Applied Systems, Inc.'s Applied Cloud System;
- Identifying, designing, implementing, operating, and monitoring effective controls over Applied Systems, Inc.'s Applied Cloud System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements; and
- Selecting the trust services categories that are the basis of our assertion.

In designing the controls over the System, we determined that certain trust services criteria can be met only if complementary user entity controls are suitably designed and operating effectively for the period November 1, 2019 to October 31, 2020.

Applied uses various subservice organizations to supplement its services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Applied, to achieve Applied's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

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 the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy, if subservice

organizations and user entities applied the complementary controls assumed in the design of Applied Systems, Inc.'s Applied Cloud System controls throughout the period November 1, 2019 to October 31, 2020.

Applied Systems, Inc.

SECTION THREE:

ATTACHMENT A: DESCRIPTION OF APPLIED SYSTEMS, INC.'S APPLIED CLOUD SYSTEM

Overview of Applied Systems, Inc.'s Operations

Applied Online™ Platform and Solutions

Since 1983, Applied Systems, Inc. ("Applied") has led an industry we helped to create with a mission to continuously improve the business of insurance. Insurance agencies and brokerages have faced new challenges and demands on their businesses over time, and we have been there to guide them. Applied has been at the forefront of insurance technology, leading the way through innovation. As the insurance industry becomes increasingly global, we are delivering new technology and expanded multinational capabilities for this changing marketplace.

Headquartered in University Park, Illinois, Applied Systems serves 15,000 clients worldwide. Applied is a leading provider of hosted software solutions, providing applications for agencies, brokers, and carriers. These software solutions are available from a combination of Applied public and private cloud services through our Applied Cloud Services ("Applied Cloud") product offerings, depending on the needs of our customers. The Applied Cloud services/hosted infrastructure and their related controls, including system redundancy, are key differentiators in providing and maintaining a high availability, 24/7 access for customers. The scope of this report covers the hosting services which houses data within our colocation environments located within the US, Canada, and the UK.

Additional data center differentiators include:

- **High Availability Platform**
  - Purpose-built data centers classified as Tier 3+ as defined by the Uptime Institute;
  - Multiple Internet connections to provide redundant Internet access for your business;
  - Excess capacity within each center to act as the disaster recovery destination for an opposing site;
  - High availability and redundancy within each site, including uninterruptable power supply and climate control;
  - Redundant firewalls and networking infrastructure; and
  - Resource pool of servers operating in a highly available cluster to allow immediate recovery for any localized failure.

- **Data Protection and Integrity**
    - All backups preformed to disk targets then replicated to the data centers, ensuring that tapes are not lost, misplaced or damaged while in transit; and
    - 24/7/365 operation, with constant monitoring and performance of first level problem resolution against the online environment.
- **Advanced Security**
    - All databases stored in the Applied Cloud environment leverage AES-256 data-at-rest-encryption (DARE) which is FIPS 140-2 certified,
    - Network monitoring and testing protect data classified as personal information (sometimes referred to as personally identifiable information or personal data).
    - Internet traffic protected by a minimum of 256-bit, bi-directional, packet-level encryption; and
    - Advanced building design protects the data center floor from exterior penetration, maintains complex video surveillance, strict access control policies and the use of mantraps, biometric systems and on-site security guards.

Applied Cloud provides your business with the flexibility, security and business continuity to drive business growth and profitability. By hosting your Applied solution in the cloud, you gain best in class technology to support online product needs. Applied Systems is committed to continually investing in the online environment to support your business growth.

Applied Cloud System Overview

Applied provides our market leading software applications, including Applied TAM, Applied Epic, Applied CSR24, Applied Mobile, Rating Services, IVANS E-Commerce Service (ECS), WARP, and other products to our customers from the Applied Cloud environment. Agency/broker management systems are provided through a Software-as-a-Service model, with customers purchasing software use rights for the number of users required. Each agency or brokerage management system has different operating requirements and is presented to the end user over the best delivery method to support a rich end-user experience.

Scope of Audit – Applied Systems Data Centers

Applied operates the Applied Cloud platform from within purpose-built colocation data centers geographically distributed to support its customers. Facilities are selected using a risk assessment process to identify locations that have a low risk of natural disaster from earthquake, flood, fire, windstorm or other severe weather conditions. Site selection also included consideration for local civil disruptions, power capacity and stability, proximity to other high risks such as railways, airports, and selective manufacturing environments. Each data center has a SOC or country equivalent conducted annually.

Each colocation facility is sited at, and managed by, a subservice organization with skilled and experienced employees to provide core facility components to Applied. These include physical security and access controls; power systems including utility power, N+1 generator power, redundant UPS systems, redundant power distribution and switching components, and redundant circuits delivered to each rack; redundant heating, ventilation, and air conditioning (HVAC) systems; dry pipe and multi-zone fire detection devices with early smoke detection capabilities; video surveillance with 24-hour monitoring; and diverse telecommunications paths into the facility.

Specific features provided by the data centers include:

- **Highly Secure Environment**
  - Multiple layers of hardened physical security;
  - 24x7x365 on-site security presence;
  - Closed-circuit television surveillance with digital storage;
  - Multiple layers of electronically controlled card access;
  - Keyed access to physical Applied Systems space;
  - Electronic key card readers; and
  - Facility verification of government issued photo IDs against approved access list.
- **Power Distribution**
  - Commercial grade high-capacity UPS system with complete isolation for redundancy;
  - Multiple 1,500+ KW generators for backup power with N+1 redundancy;
  - Minimum of five days of on-site fuel supply and extended refuel contracts;
  - Each circuit breaker backed by diverse power distribution units and diverse UPS infrastructures for the ultimate in uptime;
  - Isolated redundant UPS configuration providing industry's highest MTBF; and
  - Individual circuit load monitoring to ensure the best power management.
- **Environmental Control**
  - Temperature above floor maintained between 64 and 78 degrees; humidity maintained between 40 and 60 percent;
  - Redundant HVAC with minimum of 30 percent reserved capacity installed;
  - Sufficient air handling units for N+1 redundancy; and
  - Multiple glycol cooling units for N+1 redundancy.
- **Fire Detection/Prevention**
  - Zoned dry-piped, pre-action sprinkler system; and
  - Zoned VESDA (Very Early Warning Smoke Detection) system throughout the data center.

- **Private/Point-to-point network connectivity**
    - Applied Systems provides connectivity options for VPN solutions between Applied data center and some clients' facilities, as required; and
    - Applied Systems supports the use of MPLS connectivity into the Applied Cloud environment for customers who prefer to use network connectivity with carrier provided service level agreements.
- **Connectivity** (Availability and selection of carriers varies by location)
    - Diverse entry paths into each facility;
        - ✓ Level 3;
        - ✓ Comcast;
        - ✓ Zayo;
        - ✓ SunGard;
        - ✓ Equinix;
        - ✓ Bell CanadaPeer1;
        - ✓ BritishPeer1

Overview of the System and Applications

System Overview

The System is comprised of the following components:

- ***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);
- ***Data***: The information used and supported by a system (transaction streams, files, databases, and tables);
- ***People***: The personnel involved in the operation and use of a system (developers, operators, users, and managers); and
- ***Procedures***: The automated and manual procedures involved in the operation of a system.

Infrastructure

Each Applied Cloud environment is consistently built in our data centers with like technologies utilizing manufacturers including Cisco, Pure Storage, Dell, F5 Networks, VMware, Microsoft, and others. Applied owns and maintains all operating equipment within the contracted (colocation) space of the data center. At a minimum, all sites contain the following infrastructure:

- *Redundant power feeds from separate UPS systems to each rack;*
- *Multiple Internet providers using BGP and diverse paths for redundancy in Internet connectivity;*

- *Redundant network infrastructure including firewalls, IDS/IPS, Domain & Geolocation shunning, DDoS protection, load balancers, switches, VPN devices and routers;*
- *10 GB network connectivity support for all core devices;*
- *Fully virtualized server platform with servers in resource clusters based on load type;*
- *Physical hosts redundantly connected to SAN, network, and power components*
- *Virtual network segmentation for products and server purpose; and*
- *Remote control technologies including managed PDU's, secure console devices and remote server out-of-band management.*

Software

Applied leverages Microsoft® technologies for nearly all of our virtual machine operating systems. Authentication services are provided through Microsoft Active Directory, database services are provided through Microsoft SQL Server, and web services mostly provided through Microsoft IIS. Other operating systems may be found on specialty devices, custom hosting environments built to customer specifications, and limited infrastructure management toolsets.

Application products developed by Applied and operating from the data center include:

- *Analytics*
    - Applied Analytics - Applied Analytics is the first analytics application designed specifically to transform an agency or brokerage's data into visual business insights, looking at all aspects of an organization's business – from operational performance, to employee success, insurer relationships, and complete book of business analysis.
- *Agency and Brokerage Management Systems*
    - Applied Epic - Applied Epic is the insurance industry's fastest-growing agency and brokerage management system. Applied Epic's modern, flexible and secure architecture provides agencies and brokerages with a single platform that scales as you grow.
    - Applied TAM - Applied TAM is the most-widely used agency management software in the insurance industry for business automation. For more than 37 years, Applied TAM has provided insurance agencies and brokerages with the leading software to manage day-to-day operations across their business.
    - Applied Vision (US only) - Applied Vision is designed for agencies that manage complex business structures and complicated commercial lines of coverage, specialty lines of business or nontraditional niche markets. Applied Vision provides visibility and automation capabilities that enable agents to save time, mitigate risk and reduce operating expenses.
    - Applied DORIS (US only) - Applied DORIS is an easy-to-use online agency management system, enabling smaller agencies to remain competitive and grow their business.

- *Mobile*
    - Applied Mobile - Applied Mobile is the first independent agent mobile application designed specifically for insurance producers. With its intuitive interface, producers can access and manage client and prospect information in their agency management system through a tablet to more effectively serve clients for increased sales and customer satisfaction. Applied Mobile includes integrated productivity and risk assessment tools that maximize producers' time and service capabilities outside the agency.
    - Applied MobileInsured - Delivers accurate, convenient access to the most current insurance information at the tap of an icon. Applied MobileInsured™ is the industry's first native, branded mobile application built specifically for agencies, so customers can interact with the business when and how they prefer. Available through Applied CSR24®, the mobile app delivers the latest policy details to clients directly on their mobile device.
- *Rating Services*
    - Applied Rating Services – Applied Rating Services is a comprehensive rating services portfolio that automates rating workflows through tight integration with brokerage management systems. It improves lead management and elevates customer service through eSignature capabilities.
- *Customer Self-Service*
    - Applied CSR24 - Applied CSR24 is the on-demand customer self-service application designed to allow customers instant access to their insurance information. Its customizable and secure online platform gives agencies and brokers the ability to provide personalized online client service, resulting in increased customer retention and satisfaction, while mitigating risk and reducing operating expenses to drive sustainable growth and profitability.
- *Insurer Interface*
    - IVANS Download (US only) - IVANS Download offers batch automated updating of an agency's database with important information from carrier databases about renewals, endorsements, new business, cancellations and reinstatements for more up-to-date and efficient business transactions.
    - IVANS Real-Time (US only) - IVANS Real-Time offers real-time automated data exchange with important information from carrier databases about renewals, endorsements, new business, cancellations and reinstatements for more up-to-date and efficient business transactions.
    - Applied WARP (CN only) - Applied WARP keeps you on top of the insurance market through real-time, automated data exchange with insurers. Your brokerage will be able to respond to customer inquiries, return quotes and close sales before a prospective client leaves your office or hangs up the phone.

Data

Applied Systems acts as the data processor for agency/broker and carrier information stored or transmitted through the Applied Cloud environment. Specifics include:

- Customer data stored within the Applied Cloud environment is classified as CONFIDENTIAL to all Applied staff;
- Applied stores data in one of the aforementioned data centers, which is backed-up daily and replicated to its paired site for disaster recovery;
- In addition to stored/hosted data being encrypted at rest, Applied uses secure communications channels for data transmitted through the application or Web services between the end-user and the data center, and
- Applied destroys data from online storage after 45 days of the cancellation of a contract, and data expires from backup media in accordance with its backup retention policy.

People

The competence of employees is key element of the Applied Cloud environment. Applied is committed to the development of its employees and the recruitment of qualified professionals to support the growth of our business.

A dedicated team of technology professionals are responsible for the design, deployment, management, administration, and monitoring of the Applied Cloud environments. The data center operations team (DCO) consists of staff specializing in the storage, server, network, application, virtualization, security, monitoring, and SQL technologies. This includes engineers, application administration, a 24x7x365 operations team, and DevOps resources to create automation tools used within the data centers. All teams report up through the senior vice president of Cloud Services.

It is the responsibility of these team members to maintain the data center and the related software applications in a working state for the Applied Cloud customer base. This includes managing resources against capacity requirements, provisioning new orders, monitoring for system and application health, performing routine application updates and patch management at the OS and application layers, and monitoring for and remediating security threats.

Key positions are as follows:

Executive Vice President, Customer Experience is responsible for Applied's customer delivery strategy and operational execution for Applied's Professional Services, Support and Cloud-based solutions.

Senior Vice President of Cloud Services, heads global IT operations for Applied's Cloud Hosting and corporate IT services and oversees the operations of Applied's four global data centers.

Vice President of Information Security heads the Office of Information Security for Applied Systems. Leads all information security related initiatives, including management of the information security program, which includes formalizing a cyber-risk management strategy, continuous data mapping exercises, as well as, vulnerability management practices and incident response procedures.

Vice President of Internal Application Development directs the technology, architecture, and application development of internal and data center information systems and integrations.

Director of Internal Application Development directs the technology, architecture, and application development of internal and data center information systems and integrations.

Director of Data Center Engineering leads the team responsible for the architecture, deployment, and support of technology within the Applied Cloud data centers.

Product Manager for Applied Cloud is responsible for developing the product roadmap for Applied Cloud administration and management applications, and consulting with the Applied application development teams to represent the unique requirements that come with hosting and updating Applied applications in the data center.

Procedures

Applied provides multiple technology platform services to its customers from the Applied Cloud environment through a subscription of services. These include agency and brokerage management systems, carrier interface, reporting services, and consumer-focused products.

Applied has a series of procedures to provision new subscriptions for service provided by the Applied Cloud platform. These steps include:

- Setup new client entities based on executed services and business associate contracts;
- Provisioning of dedicated resources if subscribed to Private Cloud Services;
- Modify backup and monitoring policies to include new resources;
- Verify product access is customer ready; and
- Setup initial authorized application administration account and provide information to customer in a secure manner.

Once new system subscriptions are created and administrative users for the client account have been established within the system, the following activities occur to ensure that services are available for client use:

- Resources actively monitored for available and capacity management;
- System performance metrics reviewed;
- Backup and restore procedures performed;
- Application updates managed;

- Customer communications distributed to advise of maintenance schedules, product updates, and other relevant information;
- Ongoing security management, assessments, and remediation; and
- Termination of access when customer cancels service, including the removal of data in accordance with the defined policy after a designated holding period.

Boundaries of the System

The boundaries of the system are related to the specific aspects of the Applied Cloud platform including data centers used for hosting, the organizations hosting infrastructure, software, people, procedures, and data necessary to provide its services within the United States. The boundaries include the system administration necessary to update and maintain the Applied products and other related hosting components. The following teams are included in scope for the services provided by the Applied Cloud solution:

- **Data Center Operations**
  - DCO Engineering – responsible for core storage, server, application infrastructure design, implementation, and capacity management;
  - DCO Network Engineering – responsible for the network layer including routers, switches, firewalls, other security and network monitoring devices;
  - System Operations II – responsible for daily administration of Applied Cloud products and application updates;
  - System Operations I – responsible for the operation of the Network Operation Center (NOC), monitoring system availability, providing first level problem resolution, provisioning new orders, performing daily operational support tasks; and
  - DevOps – Dedicated development team to create automation tools utilized by DCO and customers to help manage the Applied Cloud environment.
- **Information Security and Privacy**
  - Security Analysts - Responsible for the implementation of information security policies, procedures, standards, technical safeguards, and solutions identified to mitigate or reduce business exposure to information security risks.
  - Privacy Analysts - Manage the operational risks related to privacy and sensitive information. Continuously assess business unit operations, develops policies, procedures and training; leads data mapping exercises, and other privacy related projects.
  - Security Risk and Compliance Analysts - Serves as the liaison for all IT-related security assessment functions including third-party vendor security audits, client/business partner security audits, RFP/due diligence security reviews, SOC 2 Type II audits, and any additional compliance requirements as needed.

- **Human Resources**
    - The Human Resources department is responsible for the development, administration and delivery of business solutions and programs related to Applied's Human Capital Strategy and people practices, including employee relations, policies, benefits, HRIS reporting, talent acquisition, performance management and legal compliance.

Applied Systems DCO staff does not perform or manage transaction processing, reporting, or application security on behalf of its customers. This report is, therefore, limited to those control objectives that relate to the Applied Cloud infrastructure and supporting information systems utilized by the Applied data center operations staff.

Application level security, user controls, transaction processing, reporting, and related procedures that are part of the supplied software applications provided to the Applied customer are complementary user controls and are outside of the defined boundary.

Incident Disclosure
No security incidents were detected or reported during the audit period that would affect Applied System's service commitments or system requirements.

Scope

The scope of the review is limited to the Applied Systems' System described within this "Applied Systems, Inc.'s Description of its Applied Cloud System".

Control Environment

Key facets of the Company's control environment relating to processing and staffing for all processes performed by the Company are summarized below. These areas include:

- Management Controls
- Code of Conduct
- Information Security Governance
- Security Policies and Procedures
- User Access
- Password Policies
- Remote Access
- Firewall, IDS/IPS and Anti-Virus Software
- Security Monitoring and Incident Reporting
- Physical Security and Environmental Controls
- Application and Database Architectural Development and Maintenance
- Computer Operations

- Change Management
- Backup and Recovery

The control environment reflects the overall attitude and awareness of the Board of Directors, management and personnel concerning the importance of controls and the emphasis given to controls in Applied's policies, procedures, and actions. The organizational structure, separation of job responsibilities by departments and business function, and documentation of policies and procedures are the methods used to define and implement operational controls.

Management Controls

Applied has a highly experienced management team responsible for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures. Management focuses on maintaining sound internal controls and the integrity and ethical values of all Applied personnel. Organizational values and behavioral standards are communicated to all personnel through policy statements, awareness training, and guidelines during new hire orientation and are available for review on the Applied Intranet.

Code of Conduct

Applied Systems expects all its employees and Applied representatives to support and adhere to the highest standards of business ethics and conduct. In addition, Applied Systems expects employees and Applied representatives to exercise good judgment and act professionally while on the job. A committee is responsible for the establishment, communication, investigation, and remediation of matters relating to corporate ethics. This includes, but is not limited to, fair-hiring requirements, business ethics, conflicts of interest, gifts and entertainment, anti-harassment, substance abuse, and anti-bribery. Any unethical behavior will be subject to disciplinary action up to and including dismissal from employment.

Information Security Governance

Applied has established policies and procedures that are formally documented and communicated to employees relative to information security. The Vice President of Information Security and Data Protection Officer is responsible for setting the corporate guidelines and security culture for Applied. The recommendations of the Data Protection Officer are reviewed and approved by the executive team.

Security Policies and Procedures

Information security policies are the foundation for Applied Systems' Information Security Program. Published policies have been endorsed at the highest level of management within Applied. Policies outline employee behaviors necessary for the protection of Applied information assets. Clear, consistent policies help everyone; from the executive management team to the newest employee, understand the importance of information security and what each person can do to help safeguard Applied.

A policy might have an associated standard (security control) detailing "how" to achieve the directives of the policies. In addition, platform standards specify the security configuration and administration of various computing systems including mobile devices, desktops and laptops, servers, and various networking system components (firewalls, routers, switches, etc.).

Policies are reviewed at planned intervals (no less than annually) or if significant changes occur to the environment.

User Access

Access to Applied information assets is based on the management principle of "least privilege." This principle limits access to information based on functional job roles and responsibilities that result in "need to know." Access to information content is also based upon formal roles and responsibilities established by an information owner.

Only formally authorized individuals can access information and information systems of Applied. All personnel must be identified (authenticated) prior to using any computer or network resources within the Applied Cloud. Access to networks, network services, and applications are controlled by a secure log-on procedure. Strong methods of authentication may be deemed necessary, such as the use for multifactor authentication (MFA) for remote VPN access. Documented procedures guide the addition, change, or deletion of user access upon dismissal of their employment, contract, or agreement, or adjusted upon change of job responsibility. Access rights for each user are controlled and monitored throughout a user's lifecycle with periodic reviews for accuracy and necessity occurring.

Password Policies (both internally and externally)

Passwords are currently the most common authentication used at Applied, and password security is the front line of information protection. A poorly chosen password could compromise Applied Systems' entire corporate network. All employees and third parties are responsible for selecting and securing well-chosen and complex passwords as required by policy.

Remote Access

Remote access between Applied Systems and any approved external entity, and all third-party access is controlled; access and activity are logged, monitored, and reviewed. Any such access follows a formal request process that provides for the approval and tracking of these connections. Only VPN solutions, which provide secure encrypted tunnels between locations or for users, are used for remote access.

Firewall, IDS/IPS and Anti-Virus Software

Applied Systems leverages Domain/Geo location shunning services, IDS/IPS solutions, and next generation firewalls to protect the Company servers and host systems, and to protect the network from the threats originating from the Internet. All traffic destinations and types

of traffic, both inbound and outbound, are inspected and blocked if the determined payload is malicious in nature. Protocols that are allowed through the firewalls must be specifically defined in written Firewall Rule Sets. All firewalls are configured to only allow the traffic on the approved ports.

The OIS (Office of Information Security), in conjunction with IT, has implemented procedures to check firewalls and verify that the rule sets have been accurately implemented. Firewall and IDS/IPS logs are reviewed on a regular basis for malicious activity. Firewall and IDS security logs are maintained in a way that prevents them from being modified or deleted without authorized approval.

All change requests to firewall configurations must be made to either Corporate IT or Data Center Operations and approved through a formal work order process. Firewall policies are audited and verified on a semiannual basis. The audit is conducted by personnel other than those responsible for the configuration and management of the firewall(s).

All computers attached to the Applied Cloud network must have standard, supported anti-virus software installed. This software is active, scheduled to perform virus checks at regular intervals, and is kept up to date. The anti-virus software is operated in real time on servers and client computers. The anti-virus library definitions are kept current.

Security Monitoring and Incident Reporting

Monitoring of the Applied Cloud-computing environment is intended to detect unauthorized activities. Routine monitoring, log reviews, and analysis of security incidents help identify policy violations, malicious activity, and operational problems. Logging activity provides information for incident reporting and may be mandated by certain legal and regulatory requirements.

Any employee of Applied Systems or an organization outside of Applied Systems may report a real or a suspected Security Incident. Applied Systems can also identify an incident through ongoing automated and manual network and information security activities.

Once identified, an Incident Response Team will use standard internal procedures to log and track the event and as appropriate, take steps to investigate, contain, eradicate, and remediate the incident.

Physical Security and Environmental Controls

Applied Systems protects its information assets by implementing physical, environmental, and administrative security controls at each cloud facility to guard against unauthorized access and to maintain the integrity of its information assets.

Each facility documents its building and site security requirements. OISP will collaborate with IT and DCO to develop and maintain physical and environmental controls for all Applied facilities, including collocated facilities.
These security controls include:

- Physical protection of information assets
- Management of physical access
- Environmental security
- Equipment disposal and reuse

Controls are implemented to reduce the risk of physical failure to infrastructure components, damage from natural or fabricated environmental hazards and access to Applied's information assets by unauthorized persons.

Data center security requires that all personnel entering the site must first be registered and approved. For access to Applied Systems space within one of these facilities, this requires that DCO management file an access list modification request with the employee name and duration of access prior to access being provided. Upon arrival, the guest must verify identity with the site personnel and receive access credentials valid for that visit only.

Application and Database Architectural Development and Maintenance

A business case for maintenance, development, or acquisition of information system software or hardware requires that security needs be identified, justified, agreed upon, and documented. Security requirements are identified during the project requirements definition phase and are integrated into the early stages of all information system projects. Information security controls for the system under development are included in development and quality assurance testing.

Access to system files, data base management systems, and program source code is controlled using appropriate security mechanisms and procedures. Sensitive customer information is not used in test, development, or training environments without the consent from the customer.

Computer Operations

Information processing and communication facilities must follow documented procedures for critical system operations:

- Start-up and shutdown procedures
- System backup
- Equipment maintenance
- Media handling
- Computer rom and mail handling management
- Safety

Systems management takes reasonable measures for verifying that operating procedures are done consistently.

Change Management

Changes, upgrades, and patches to systems, networks, applications, and databases at Applied are authorized and must follow a documented change control process. The documented change management procedures cover emergency changes as well as standard changes.

Unique, separated environments for production and non-production (development, test, quality assurance) operations reduce the risks of inadvertent or unauthorized access or changes to production data or systems.

Backup and Recovery

Applied Systems recognizes that Business Continuity (BC) and Disaster Recovery (DR) Planning are essential management processes to minimize the negative effects of a major business disruption created by a disaster or failure.

The BC/DR management process identifies potential threats and provides a roadmap for an effective response that mitigates or minimizes the exposure of the Applied's assets to unexpected interruption. Applied Systems emphasizes the importance of an established BC/DR program that safeguards the interests of Applied, stakeholders and its customers.

Applied Systems' business continuity and disaster recovery plans include clear strategies and procedures needed to continue operations and execute a recovery in the event of an interruption that compromises the ability of Applied Systems to perform its critical business processes. Applied Systems inventories the information technology resources (equipment, software, etc.) and identifies the resources needed to support essential functions. Applied Systems periodically tests and reviews BC/DR plans to verify that they are adequate. Applied has developed processes for creating copies of critical data that are stored at an approved, redundant backup location with appropriate access controls and storage procedures.

Risk Assessment

Applied Systems employs both formal and informal risk assessment procedures. Security efforts within Applied Systems address risks in an effective and timely manner where and when they are needed. Information security risk management is a continual process which assesses and treats risks using a risk treatment plan. A formal security risk assessment is conducted annually by OIS. The process includes identifying, prioritizing, and ranking risk at both the entity and activity level.

Applied Systems performs risks assessments of potential operational risks which may impede achieving the control objectives covered by this report. In addition, Senior Leadership meets on a frequent basis with leadership teams and staff to discuss business operations and

identify areas which may indicate a problem. Remedial action plans are designed and implemented to mitigate the likelihood of risk occurrence. Applied Systems management emphasizes risk awareness in order to effectively identify, monitor, and manage risks that could adversely affect Applied's ability to provide reliable hosting solutions to its customers. The primary risks that have been identified through this process pertain to Human Resources management, corporate and customer system security, availability, and confidentiality, network infrastructure, and physical and logical access rights.

Significant System and Control Changes

The IT environment has been stable throughout the period and there have been no significant changes to the system. The description does not omit or distort information relevant to Applied System's system. Applied System acknowledges 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.

Monitoring

The CTO & CIO monitor the quality of internal control performance as a normal part of their activities. They are heavily involved in day-to-day activities and regularly review various aspects of internal and customer-facing operations to (i) determine if objectives are achieved, (ii) identify any new risks that develop, and (iii) implement appropriate measures to address those risks. XYZ adopts a proactive approach to the monitoring of application security to ensure that any issues or risks are addressed before becoming significant problems.

Monitoring of the Subservice Organizations

Applied uses various subservice organizations to supplement its services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Applied, to achieve Applied's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

Information and Communication

Computerized Information Systems

Each Applied Cloud environment is consistently built in our data centers with like technologies utilizing manufacturers including Cisco, Pure Storage, Dell, F5 Networks, VMware, Microsoft, and others. Applied Systems owns and maintains all operating equipment within the contracted (colocation) space of each data center.

Applied Systems leverages Microsoft® technologies for nearly all of our virtual machine operating systems. Authentication services are provided through Microsoft Active Directory, database services are provided through Microsoft SQL Server, and web services mostly provided through Microsoft IIS. Other operating systems may be found on specialty devices, custom hosting environments built to customer specifications, and limited infrastructure management toolsets.

Communication

Management is committed to maintaining effective communication with all personnel. Data Center Management meets weekly to discuss the status of service delivery or other matters of interest and concern. Issues or suggestions identified by personnel are readily brought to the attention of management to be addressed and resolved.

Notification of scheduled changes is communicated to an inter-departmental change advisory board on a weekly basis. On a quarterly basis, operating performance reports are provided to senior management to summarize the performance statistics of the various Applied Cloud products.

Applied has established policies and procedures that are formally documented and clearly communicated to all employees. Written position descriptions and other policies and procedures communicate the responsibility to appropriately communicate significant issues and exceptions in a timely manner.

Description of Complementary User Entity Controls

Applied Infrastructure controls were designed with the assumption that certain controls would be implemented by user entities (or "customers"). Certain requirements can be met only if complementary user entity controls assumed in the design of Applied Infrastructure's controls are suitably designed and operating effectively, along with related controls at Applied Infrastructure.

SECTION FOUR:

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Applied Systems Inc. describes the services and scope of work provided to its clients through Applied software and services agreements and the organization's public website. Services and responsibilities are documented and agreed upon by both parties in the Applied Master Agreements, and contracts must be established before services are provided. Applied designs its software solutions to meet contractual commitments. These commitments are based on the services that Applied provides to its clients.

Security commitments are documented and communicated to customers within these agreements, which include, but are not limited to, the following:

- Use of encryption technologies to protect customer data both at rest and in transit
- Use of firewalls, IP shunning, and network segmentation restricting traffic flow
- Security monitoring infrastructure including intrusion detection, centralized log management, and alerting
- Geographically separated data center with multi-layered physical security controls
- Vulnerability Management program designed to identify and correct vulnerabilities within the environment in a timely manner
- Incident Response program designed to minimize the impact and protect resources