EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed.
   (i) Complaints should be submitted to the EA at: CA BOCES Data Privacy Officer, 1825 Windfall Road, Olean, New York 14760, via email at DPO@caboces.org or by using the form available at the following website: https://caboces.org/resources/new-york-state-education-law-2d/report-an-improper-disclosure/.
   (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
Signature:	
Printed Name:	Joshua R. Dunnill
Title:	Director of EHR Go
Date:	4/9/24

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	EHR Go
Description of the purpose(s) for which Contractor will receive/access PII	Meta data on user interaction with application.
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII □ APPR Data
Contract Term	Contract Start Date 4/9/2024 Contract End Date 4/8/2025
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) □ Contractor will not utilize subcontractors. ☑ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties**.** • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.

Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☑ Using a cloud or infrastructure owned and hosted by a third party. □ Using Contractor owned and hosted solution □ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Data encrypted at rest and in transit using industry standard procedures. All data hosted by Atomic Data who holds both a SOC 2 and 3 certification.
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
Signature:	Joshua R
Printed Name:	Joshua R Dunnill
Title:	Director of EHR Co
Date:	4/9/24

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	All items handled through Atomic Data, our third party hosting provider. See provided SOC3 report.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	All items handled through Atomic Data, our third party hosting provider. See provided SOC3 report.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	All items handled through Atomic Data, our third party hosting provider. See provided SOC3
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All items handled through Atomic Data, our third party hosting provider. See provided SOC3
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	All items handled through Atomic Data, our third party hosting provider. See provided SOC3 report
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	All items handled through Atomic Data, our third party hosting provider. See provided SOC3 report.
7	Describe your secure destruction practices and how certification will be provided to the EA.	All items handled through Atomic Data, our third party hosting provider. See provided SOC3 report.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	All items handled through Atomic Data, our third party hosting provider. See provided SOC3 report.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	

Function	Category	Contractor Response
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	

Function	Category	Contractor Response
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

April 16, 2022 to April 15, 2023

Table of Contents

SECTION 1

ASSERTION OF ATOMIC DATA, LLC MANAGEMENT

ASSERTION OF ATOMIC DATA, LLC MANAGEMENT

May 1, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within Atomic Data, LLC's ('Atomic Data' or 'the Company') Managed Services System throughout the period April 16, 2022 to April 15, 2023, to provide reasonable assurance that Atomic Data's 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*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Atomic Data, LLC's Description of Its Managed Services System throughout the period April 16, 2022 to April 15, 2023" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 16, 2022 to April 15, 2023, to provide reasonable assurance that Atomic Data's service commitments and system requirements were achieved based on the trust services criteria. Atomic Data'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 "Atomic Data, LLC's Description of Its Managed Services System throughout the period April 16, 2022 to April 15, 2023".

Atomic Data uses Databank Holdings, Ltd. ('Databank') to provide colocation, environmental infrastructure, and preventative maintenance services and Cologix to provide telecommunications services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Atomic Data, to achieve Atomic Data's service commitments and system requirements based on the applicable trust services criteria. The description presents Atomic Data's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Atomic Data's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Atomic Data's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Atomic Data's controls.

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 April 16, 2022 to April 15, 2023 to provide reasonable assurance that Atomic Data's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Atomic Data's controls operated effectively throughout that period.

Dwayne Sapp

Dwayne Sapp
General Manager
Atomic Data, LLC

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Atomic Data, LLC:

Scope

We have examined Atomic Data accompanying assertion titled "Assertion of Atomic Data, LLC Management" (assertion) that the controls within Atomic Data's Managed Services System were effective throughout the period April 16, 2022 to April 15, 2023, to provide reasonable assurance that Atomic Data's 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*, in AICPA *Trust Services Criteria*.

Atomic Data uses Databank to provide colocation, environmental infrastructure, and preventative maintenance services and Cologix to provide telecommunications services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Atomic Data, to achieve Atomic Data's service commitments and system requirements based on the applicable trust services criteria. The description presents Atomic Data's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Atomic Data's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Atomic Data, to achieve Atomic Data's service commitments and system requirements based on the applicable trust services criteria. The description presents Atomic Data's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Atomic Data's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

The information included in Section 4, "Other Information Provided by the Service Organization," is presented by Atomic Data management to provide additional information and is not a part of the description. Information about Atomic Data's announcement regarding interim leadership moves has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Atomic Data's service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

Atomic Data is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Atomic Data's service commitments and system requirements were achieved. Atomic Data has also provided the accompanying assertion (Atomic Data assertion) about the effectiveness of controls within the system. When preparing its assertion, Atomic Data 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 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 AICPA. 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 the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its 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.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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 Atomic Data's Managed Services System were suitably designed and operating effectively throughout the period April 16, 2022 to April 15, 2023, to provide reasonable assurance that Atomic Data's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Atomic Data's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Atomic Data's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Atomic Data, user entities of Atomic Data's Managed Services System during some or all of the period April 16, 2022 to April 15, 2023, business partners of Atomic Data subject to risks arising from interactions with the Managed Services System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

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

A-LIGN ASSURANCE

Tampa, Florida
May 1, 2023

SECTION 3

ATOMIC DATA, LLC'S DESCRIPTION OF ITS MANAGED SERVICES SYSTEM THROUGHOUT THE PERIOD APRIL 16, 2022 TO APRIL 15, 2023

OVERVIEW OF OPERATIONS

Company Background

Atomic Data is a privately-owned company with headquarters located at 250 Marquette Avenue South in Minneapolis, Minnesota. Atomic Data also has an additional office location located at 750 B Street in San Diego, California. Jim Wolford and Larry Patterson founded Atomic Data in 2001.

Atomic Data is a provider of a wide range of managed infrastructure and enterprise Information Technology (IT) services. Atomic Data manages four data center facilities worldwide, with a core group of three data centers in the Minneapolis area.

Atomic Data connects its data centers with redundant 10-gigabit fiber links and numerous Internet connections with major international Internet Protocol (IP)-transit providers. Atomic Data partners with local exchange carriers and infrastructure providers to bring last-mile connectivity back to an Atomic Data-managed national multi-protocol label switching (MPLS) wide-area network (WAN). This flexibility allows Atomic Data to host high-availability web sites, applications, enterprise-WAN networks, and Voice over IP (VoIP) services for its clients.

Atomic Data monitors and manages its services from its 24x7 Network and Security Operations Center (NSOC), from which aspects of the data center environments, network conditions, and hosting systems health are measured. The Atomic Data Client Support and NSOC teams combine to provide 24x7 managed help desk and other custom management services.

Atomic Data has a dedicated Internal Security and Compliance team which sets a high standard for security controls and provides guidance for management in evaluating and remediating security risks. Oversight boards provide formal governance and approval to proposed changes, including services, policies, organizational changes, ongoing risk management, and changes to the Atomic Data Network Control Environment.

Description of Services Provided

Atomic Data offers a complete suite of managed technology services that provide clients with the building blocks for enterprise class infrastructures. These services include:

1. The Atomic Cloud®
2. Data Center Colocation
3. Enterprise Architecture and Implementation
4. Security & Compliance Consulting
5. 24x7 Network Monitoring & Management
6. 24x7 Technical Support
7. Orange Book - Annual IT Asset Review and Budget Planning
8. Server and Workstation Management
9. Remote Data Backup and Disaster Recovery Products
10. Connectivity and Internet Service Provider (ISP) Services
11. Hosted Solutions
12. Web and Software Development
13. Software and Platform Optimization Services

The Atomic Cloud®

Atomic Data helps clients build a cloud solution that leverages existing IT resources and aligns with a client's specific needs. Atomic Data's virtual server environments allow companies to consolidate multiple applications and operating systems to run on a single physical server. Virtual Server environments enable companies to utilize available server capacity while providing critical applications with additional resources during peak times. Clients may purchase Atomic Data monitoring and Atomic Data patch-management services for their virtual servers. Atomic Data patches, monitors, and manages Windows and Linux virtual servers with a variety of enterprise management software suites.

Data Center Colocation

Atomic Data's global facilities are built for maximum uptime, connectivity, and redundancy. Atomic Data offers data center colocation combined with engineers, partnerships, and all-encompassing service packages.

Available from 1U to multi-rack and private cage configurations, colocation allows small and midsize businesses to cost-effectively house their voice, computing, and networking equipment within a highly connected, secure facility equipped with numerous layers of redundancy, monitoring, and environmental controls. Colocation is also ideal for creating a centralized computing location for companies with distributed physical locations.

Atomic Data directly controls and manages the MSP250 data center suite and services provided at the facility. Atomic Data directly controls and manages the colocation services provided at the MSP7700 and DFW400 data centers, while utilizing DataBank as a subservice organization for facility infrastructure.

Enterprise Architecture and Implementation

Atomic Data's vast, proven enterprise experience and deep bench of industry-certified engineers and architects work closely with Atomic Data's Architecture and Implementation services. Enterprise Architecture and Professional Services implementations include WAN Design, Local Area Networks (LAN) Design, cloud architecture and migration planning, storage evaluation and recommendations, disaster recovery playbooks, and more. Enterprise Implementation services are tailored to meet clients' specific technology needs.

Security and Compliance Consulting

The safety and security of client data is Atomic Data's highest priority. Whether Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), or SOC 2, Atomic Data's industry-certified security and compliance professionals help clients safeguard their data by assisting them in implementing managerial oversight, comprehensive policies and procedures, physical and logical access controls, computing/software/network controls, and data destruction techniques to prepare for a multitude of industry-specific security and compliance audits.

24x7 Network Monitoring and Management

Atomic Data's NSOC is just a phone call, email, or support portal ticket away. Using a selection of industry-standard monitoring platforms combined with customized solutions, Atomic Data's NSOC technicians monitor client networks 24x7 to identify and resolve network issues to prevent downtime. In addition to monitoring data centers, routers, switches, servers, applications, storage networks, and websites, Atomic Data's NSOC also manages incident response, serving as the first line of defense when issues arise.

24x7 Technical Support

Atomic Data offers 24x7 email, phone, and web portal-based support for a client's employees, executives, and even their clients. Atomic Data's Client Support and on-site services are ideal for augmenting or replacing IT resources for businesses looking to eliminate the burden and cost of maintaining an internal IT staff, keeping up with growth, industry trends, or workload. From software, hardware, peripherals, to Virtual Private Network (VPN) access, and more, Client Support remotely assists with a wide array of issues and is often the primary point of contact for many of Atomic Data's clients. For more complex issues or those that cannot be resolved remotely, Client Support escalates to the appropriate department for resolution.

Orange Book - IT Asset Review and Budget Planning

The Orange Book is a comprehensive document that provides insight into aspects of the current state of a client's IT environment and how specific areas are performing. Atomic Data uses the Orange Book to inventory and assess switches, routers, workstations, printers, servers, backup systems, software assets, user accounts, and more. The Orange Book gives clients a useful first step in defining a custom maintenance schedule, future state upgrades, and IT-related financial planning that fits their network's specific components and complements their business plan.

Server and Workstation Management

Atomic Data takes on the burden of patching, securing, monitoring, and auditing servers and workstations using advanced management tools to save clients time and money. Clients can rest assured that mission critical servers and desktops are under the competent and watchful eye of Atomic Data's 24x7 NSOC and Client Support teams. Server and workstation management also includes patch management, endpoint antivirus, auditing, remote access, automated procedures, system imaging, and agent/system logging.

Remote Data Backup and Disaster Recovery Products

Atomic Data provides backup products and the expertise to help ensure the safety of client's critical data. Multi-level backup options for workstations, laptops, servers, and cloud solutions allow clients to configure a secure, cost-effective backup scheme tailored to their specific business needs. Atomic Data also offers disaster recovery options tailored to balance client budget and risk management requirements. From off-site data backup to a fully equipped secondary site, Atomic Data's data security consultants help clients choose the option that best meets their needs.

Connectivity and ISP Services

At the foundation of Atomic Data's managed ISP services are numerous 10-gigabit border gateway protocol (BGP) peers, which provide high-capacity, redundant, multi-homed internet availability for clients and services within the Atomic Data network. Atomic Data's data centers are interconnected with 10-gigabit fiber links, providing redundant, transparent networking between facilities. For managed ISP connectivity services, Atomic Data offers a full range of bandwidth circuits, including 10 Mbps and up metro-ethernet circuits, traditional circuits such as Digital Signal 3s (DS3s) and T-Carriers (T1s), and digital subscriber line (DSL), of which may be used to build private MPLS-based WANs. To augment traditional telco connections for failover and/or flexibility purposes, Atomic Data also offers managed encrypted WAN services, including Internet Protocol Security (IPSEC) VPN, Secure Sockets Layer (SSL) VPN, IPSEC VTI, Dynamic Multipoint Virtual Private Network (DMVPN), and software-defined networking in a wide area network (SDWAN) services to enable customers using a third-party ISP secure, private connectivity to Atomic Data's infrastructure.

Hosted Solutions

From Microsoft Exchange to DNS and web hosting, Atomic Data provides businesses with enterprise-grade hosting services that feature security, reliability, and support. Atomic Data offers highly available and secure hosted solutions that not only eliminate the need for large capital expenditures, but also removes the burden of server maintenance and administration.

Web and Software Development

Atomic Data's Software Development team does everything from SharePoint customizations to proprietary .NET applications and structured query language (SQL) database clustering. By partnering with business stakeholders and IT resources, Atomic Data's Software Development team leverages software to enable clients to be more competitive and operate more efficiently.

Atomic Data's software architects and business analysts engage with clients at the front end of the software development lifecycle (SDLC) to design custom software solutions catered to an organization's business needs. Upon completion of application architecture and design, Atomic Data drives development through an iterative development process that follows the Agile software development methodology, aligning with client timeline and budget goals. Atomic Data provides flexible application development options, including complete software development services, hybrid development teams that include internal client employees, and simplified leadership and mentoring of client development teams by Atomic Data's senior software architects.

In addition to development of new software applications, Atomic Data's Software Development team provides ongoing maintenance, support, and iterative development for existing applications, including applications written by third-parties. Atomic Data's Software Development team engages with a client at any point of the SDLC and custom-tailor software services for a client.

Software and Platform Optimization Services

Atomic Data provides infrastructure as a service for large software platforms and clients serving high-volume, public facing websites. Atomic Data's shared web application infrastructure supports millions of transactions per day. Atomic Data's software and platform optimization engineers assist clients in managing the deployment and ongoing monitoring and maintenance of client applications in this shared infrastructure. These services include infrastructure capacity management and performance monitoring; large volume transactional database architecture, design, and optimization; database and query optimization; application code review and optimization; high availability architecture and scaling design; managed code repositories and deployment; managed private cloud; and maintenance development services. Atomic Data's Software Development and Professional Services and Engineering teams ensure that client applications are always running at their peak efficiency within Atomic Data's shared infrastructure.

Principal Service Commitments and System Requirements

Atomic Data designs their processes and procedures to meet the objectives set for Managed Services System products and services. Those objectives are based on the service commitments that Atomic Data makes to user entities, the laws and regulations that govern the provisioning of Managed Services System, and the financial, operational, and compliance requirements that Atomic Data has established for the services.

Security commitments to clients are documented and communicated in Master Services Agreements (MSAs) and other client agreements, as well as in the description of the service offering provided to clients. Security commitments are standardized and include, but are not limited to, the following:

- Implementing the principle of least privilege for access to client systems and data
- Utilizing encryption to protect client data
- Ensuring client data is available within stated service commitments

Atomic Data establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Atomic Data's system policies and procedures, system design documentation, and contracts with clients. Information security policies define an organization-wide approach to how systems and data are protected, including how services are designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of Managed Services System products and services.

Components of the System

The system is comprised of the following:

- Infrastructure
- Software
- People
- Policies and Procedures
- Client Data

Infrastructure

Atomic Data operates within the following office and data center facilities:

- MSP250
- MSP7700
- DFW400
- MSP511

<u>MSP250</u>

MSP250 is the location of several of Atomic Data's facilities, including headquarter offices, the Network and Security Operations Center, Client Support, and the primary data center. These facilities occupy parts of a multi-tenant building at 250 Marquette Avenue South in Minneapolis, Minnesota. In tandem with building management, this facility provides 24x7 physical security, including security cameras, individually locking cabinets and cages, multi-factor card-key access, and on-site security guards.

The MSP250 data center provides secure, controlled space with redundant network access for colocation equipment. Clients may choose from a wide range of space offerings including partial, full, and multiple racks; dedicated cages; and dedicated suites. Atomic Data also operates its cloud offerings from this space, providing a highly available cloud for clients to locate their services and systems.

<u>MSP7700</u>

MSP7700 is the location of one of Atomic Data's colocation data centers. The facility is located at 7700 France Avenue South, in Edina, Minnesota. Atomic Data leases colocation space from Databank, who operates the facility. As a subservice organization, Databank operates the physical security controls around access to the facility, and environmental controls and monitoring of the facility. Specifics of the controls Databank operates are detailed in the "Subservice Organizations" section below. Atomic Data operates additional physical security and environmental controls within the leased space.

The MSP7700 data center provides secure, controlled space with redundant network access for colocation equipment. Clients may choose from a wide range of space offerings including partial, full, and multiple racks. Atomic Data operates its cloud offerings from MSP7700, providing clients with another option to locate their services and systems.

DFW400

DFW400 is the location of one of Atomic Data's colocation and cloud data centers. The facility is located at 400 South Akard Street, in Dallas, Texas. Atomic Data leases colocation space from Databank, who operates the facility. As a subservice organization, Databank operates the physical security controls around access to the facility, and environmental controls and monitoring of the facility. Specifics of the controls Databank operates are detailed in the "Subservice Organizations" section below. Atomic Data operates additional physical security and environmental controls within the leased space.

The DFW400 data center provides secure, controlled space with redundant network access for colocation equipment. Clients may choose from a wide range of space offerings including partial, full, and multiple racks. Atomic Data operates its cloud offerings from DFW400, providing clients with another option to locate their services and systems.

MSP511

MSP511 is the location of Atomic Data's network interconnection data center. The facility is located at 511 11th Avenue South, in Minneapolis, Minnesota. Atomic Data leases cabinet space from Cologix, who operates the facility. As a subservice organization, Cologix operates the physical security controls around access to the facility, and environmental controls and monitoring of the facility. Specifics of the controls Cologix operates are detailed in the "Subservice Organizations" section below.

The MSP511 data center provides Atomic Data with diverse path network interconnections between its other data centers and Internet Service Providers.

Software

Atomic Data considers the specifics of the software they use to offer their services to be proprietary and confidential. Any specific questions can be answered during an in-person review of this report.

People

Atomic Data is organized into functional areas supporting general business administration and technical operations under the executive leadership of CEO Jim Wolford. Business administration teams include Internal Security and Compliance, Communications, Sales, Accounting, and Human Resources. Technical operations teams include Client Security and Compliance, Client Engagement and Implementation, Client Support, Network and Security Operations Center, Professional Services and Engineering, Infrastructure Engineering, Product Operations, Architecture, and Software Development.

Policies relating to appropriate business practices, knowledge, and experience of key personnel are taken into consideration when defining the organizational structure. In addition, policies are established, and communications are directed at ensuring personnel understand Atomic Data’s objectives, how individual actions interrelate and contribute to those objectives, and recognize how and for what personnel will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.

Functional Responsibilities

Atomic Data assigns personnel to departments organized around technical and professional responsibilities. As a human control, these departments form the basis for the role separation found in the implementation of logical and physical controls elsewhere in the environment. This clear identification of departments and their related roles promotes efficiency, limits broad exposure, and provides for a system of internal checks and balances. Primary roles and responsibilities for each of these departments are described here.

Internal Security and Compliance

The Internal Security and Compliance department operates as the information security focal point for the organization and is responsible for the operation, maintenance, and improvement of Atomic Data's internal control environment. Internal Security and Compliance works directly with individual departments, providing clarification and guidance on policies, procedures, change management, and potential impacts to the security, availability, and confidentiality of Atomic Data computing infrastructure.

The Internal Security and Compliance department is also responsible for ongoing management and governance of Atomic Data's compliance initiatives, in coordination with Human Resources and the CEO. This includes management of the Service Organization Control (SOC) program and oversight of the supporting controls. Examples of these responsibilities include security testing; security incident investigation and analysis; developing and conducting information security awareness training and testing; monitoring adherence to organizational controls; assessing the need for changes to controls based on organization growth and changing security landscape; serving as an authoritative body to the organization on the implementation of controls; and responding to third-party audit requests.

Communications

The Communications department is responsible for Atomic Data's public image and message through a variety of channels including the atomicdata.com website, social media, e-mail campaigns, radio and television marketing, product and service marketing literature, video productions, events, press releases, and more. The department uses these channels to generate leads and attract new business. The department is also responsible for overseeing the usage of licensed images and assets on behalf of Atomic Data.

Sales

The Sales department is responsible for lead generation and new business development, as well as completing contract agreements with clients, evaluating the existing client base for additional sales opportunities, and preparing and delivering eQuotes, proposals, and completed responses to RFIs and RFPs. In addition, the Sales department places and tracks pending connectivity and power circuit orders, fulfills and tracks hardware and software orders, and distributes and maintains hardware and software inventories. New contract agreements, orders, purchases, and responses to RFIs and RFPs must be entered into the system to be fulfilled and require proper senior management authorization.

The Sales department maintains client relations and develops and maintains strategic partnerships and relationships with complementary vendors and strategic resellers to sustain the growth of Atomic Data's market share, profitability, and success.

Accounting

The Accounting department is responsible for the financial affairs of Atomic Data and preparing financial analyses of operations, including interim and final financial statements with supporting schedules for management guidance. This department manages the day-to-day accounting operations, including payables and receivables, and oversees internal financial controls, ensuring accuracy, timely deliverables, and compliance.

Human Resources

The Human Resources (HR) department is responsible for the overall acquisition, development, and retention of employees and contractors. HR works with department managers to identify staff and contractor needs, outline and maintain job descriptions, and facilitate candidate searches through recruiting activities and the interview process. Benefits development, in coordination with the CEO, is another key element supporting recruiting, development, and retention activities. In addition to onboarding new resources, HR is responsible for the ongoing development and management of the employee handbook, personnel-specific policies and procedures, and training programs for employees and contractors.

Additionally, annual background checks are required and maintained on file for employees and contractors.

Client Security and Compliance

The Client Security and Compliance (CSC) department is responsible for improving client security posture and strengthening their overall IT hygiene. This involves offering comprehensive policy and procedure development, security awareness training and phishing simulations, vulnerability scanning and management, and Security Operations Center as a Service (SOCaaS). The CSC ensures that security recommendations help clients meet industry standard compliance requirements.

Client Engagement and Implementation

The Client Engagement and Implementation departments are responsible for ensuring that information technology projects are conducted in a disciplined, well-managed, and consistent manner that assures the delivery of quality products and services. This involves appropriate planning, scheduling, and control within Atomic Data projects and ensuring efficient use of resources and tools. This department is responsible for communicating and managing client project plans, timelines, and events and obtaining client feedback upon the implementation of products and/or services.

Client Support

Client Support provides 24x7 troubleshooting of client technical issues received via phone, e-mail, and the online ticket portal. Client Support creates a ticket for each issue received. Client Support specialists and technicians use their knowledge, manuals, and troubleshooting guides to resolve the issue or determine if the issue needs to be escalated to a Level II or Level III engineer for resolution.

Network and Security Operations Center (NSOC)

The NSOC is responsible for responding to any potential issues related to Atomic Data products and services. The NSOC responds to information received by initiating tickets, performing initial triage, and escalating to the appropriate resource. The NSOC is the first point of contact for many clients and helps management monitor company trends. The NSOC is responsible for the day-to-day monitoring, maintenance, and administration of Atomic Data and client circuits, internal networking devices, NSOC management systems, and servers.

Additionally, a core group of individuals on the NSOC team are trained to identify and respond to security incidents, operating as a Security Operations Center team within the NSOC. This team meets regularly with CSC department members and assists with optimizing processes regarding identifying and responding to security events.

Professional Services and Engineering

The Professional Services and Engineering department is responsible for direct support of workstations, servers, and local, on-site networks. This team handles the maintenance and architecture for client Windows domains. Client Support provides Level I support to on-site clients. The Professional Services and Engineering department receives escalations from the Client Support and NSOC teams.

Infrastructure Engineering

The Infrastructure Engineering department is comprised of Infrastructure and Data Center engineers. The department manages Atomic Data's IP transit network, IP address allocations, ISP services, colocation facilities, and client move-ins at the data centers. The Infrastructure Engineering department receives escalations from the NSOC and Client Support teams.

Product Operations

Product Operations engineers are responsible for the architecture and maintenance of Atomic Data's virtual server infrastructure, including VMware clusters, SAN storage, and load balancers. Product Operations engineers also manage Atomic Data’s platform for agent-based remote administration, which provides patch management and monitoring for Atomic Data and client resources, as well as Atomic Data’s Black Box product and tape backup services. The Product Operations department receives escalations from the NSOC and Client Support teams.

Architecture

The Architecture department is responsible for designing and implementing data center networks that include server virtualization, LAN, WAN, intranets, extranets, network and server security, load balancing, and storage. The architects also perform system design, analysis, and planning; design network and computer security measures; and research and recommend network and data communications hardware and software. They also work with clients to design and architect custom solutions to meet the client’s unique business needs.

Software Development

Atomic Data’s Software Development department does everything from CMS and SharePoint customizations to proprietary .NET business applications and SQL database tuning and clustering. By partnering with business stakeholders and IT resources, Atomic Data’s Software Development team leverages software to enable clients to be more competitive and operate more efficiently.

Atomic Data’s software architects and business analysts engage with clients at the front end of the SDLC to design custom software development catered to an organization’s business needs. Upon completion of application analysis and design, Atomic Data drives development through an iterative development process that follows the Agile software development methodology, aligning with client timeline and budget goals. Atomic Data provides flexible application development options, including complete software development services, hybrid development teams that include internal client employees, and simplified leadership and mentoring of client development teams by senior Atomic Data software architects. In addition to development of new software applications, Atomic Data’s Software Development team provides ongoing maintenance, support, and iterative development for existing applications, including applications written by third-parties. Atomic Data’s Software Development team will engage with a client at any point of the SDLC and custom-tailor software services for a client.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, data security, and risk management. Personnel are expected to adhere to Atomic Data's policies and procedures that define how services should be delivered. These are located on the Company’s intranet and can be accessed by any Atomic Data team member.

Physical Security

Physical security controls aim to ensure the integrity of the physical environments involved in generating the service provided by Atomic Data. At Atomic Data offices, these protections include 24-hour video surveillance and recording, proximity-card controlled perimeter doorways, and punch-code secured interior doorways, which limit access to key storage areas to appropriate personnel. At the data centers, Atomic Data implements controls and policies that can function standalone when in sole control and as a complement to the controls of a subservice organization where Atomic Data does not control the entire facility. Some of the common expectations include 24-hour, multi-factor access to the facility and cages for authorized Atomic Data personnel and clients, comprehensive monitoring of internal and external environmental conditions, and extensive video surveillance.

Atomic Data also operates in facilities owned by Cologix and Databank. As such, some of the physical and environmental equipment protections are the responsibility of Cologix and Databank. For a listing of controls implemented by Cologix and Databank, please refer to the ‘Subservice Organizations’ section below.

Logical Access

Logical access controls provide directives for implementing policies and procedures that ensure the operating environment is properly secured from network or any other electronic access. Activities within the operating environment are properly authorized and documented. The primary framework for authenticating and authorizing administrative access is the Atomic Network Control Environment (ANCE). The ANCE relies principally on a user’s Active Directory (AD) account, which is required to gain access to any privileged network within the office or in conjunction with multifactor authentication for remote access. Administrative interfaces are restricted to Atomic Data-controlled access, and the level of authorization is determined on a per-user basis at every administrative interface. The ANCE is monitored in multiple ways to ensure configuration integrity and detect internal and external threats.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Atomic Data monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Atomic Data evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space, power, and cooling
- Disk storage
- Tape storage
- Network bandwidth

Atomic Data has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended patches. Clients and Atomic Data system owners review proposed patches to determine whether the patches are already applied. Clients and Atomic Data systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Atomic Data staff validate that patches have been installed and, if applicable, that reboots have been completed.

Part of the infrastructure supporting the Managed Services System is hosted within DataBank and Cologix facilities. As such, some of the environmental equipment protections are the responsibility of DataBank and Cologix. For a listing of controls implemented by DataBank and Cologix, please refer to the Subservice Organizations section below.

Change Control

Atomic Data's Change Management Board (CMB) is responsible for ensuring that change management policies and procedures are adhered to for changes to Atomic Data internal and client infrastructure. The CMB reviews planned changes to Atomic Data’s systems and network infrastructure to ensure that such changes meet requirements set forth in Atomic Data’s change management policies and client change management policies, where applicable. The CMB has authority to approve operational level changes to systems and network infrastructure. The CMB reviews previously executed changes to ensure consistency with process and identify any areas for improvement or potential problems. The CMB reviews operational events and outages to determine if they were the result of unplanned changes or could be mitigated through additional planning or change management processes.

Software Development Life Cycle

Atomic Data maintains documented SDLC policies and procedures to guide personnel in documenting and implementing application changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance (QA) testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality Assurance (QA) testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Communications

Atomic Data uses various means of communication to ensure that employees understand their individual roles and responsibilities for providing services to clients and promoting timely notification of significant events. Continuous communications and hands-on training ensure that employees are aware of important policy changes, as well as organizational changes and events. Employees are encouraged and expected to communicate new, relevant information and exceptions arising from their individual job activities, observations of internal business operations, and the external environment. Managers from departments are expected to respect the value of such communication and respond appropriately.

The Client Support and NSOC teams prepare reports at each shift change, which include important information about products and services, alerts, clients, and internal tasks relevant from the past 24 hours. Designated departments review these reports and are expected to communicate perceived possible risks and offer recommendations towards resolution, prevention, or mitigation. Management uses these reports as major inputs to Atomic Data's internal quality control.

Atomic Data has developed a system that integrates numerous technical monitoring methods designed to provide early detection and immediate response to evolving risks in the operating environment. This system is monitored 24x7 by the Client Support and NSOC teams, which identify, communicate, ticket, triage, and escalate warnings and critical alerts as appropriate. The system provides a complete overview of performance objectives at key levels including monitoring the physical data centers through cameras and environmental sensors; the hardware and operating system status of infrastructure servers and services through passive and active monitoring; as well as televised and automatic weather reporting for the local area and for the specific geographic locations of client points of operation throughout the country. Technical personnel contribute to the constant evolution and improvement of the overall system and are expected to be available 24 hours a day for escalations.

Client Data

Client data, as defined by Atomic Data, may constitute the following, depending on the services provided to the client:

- Network and system architecture diagrams
- Network device configuration files
- Application source code
- Client e-mails (e.g., if a client is using a hosted Exchange product)
- Client system images and data
- Policies and procedures
- Incident details
- Vulnerability scan data

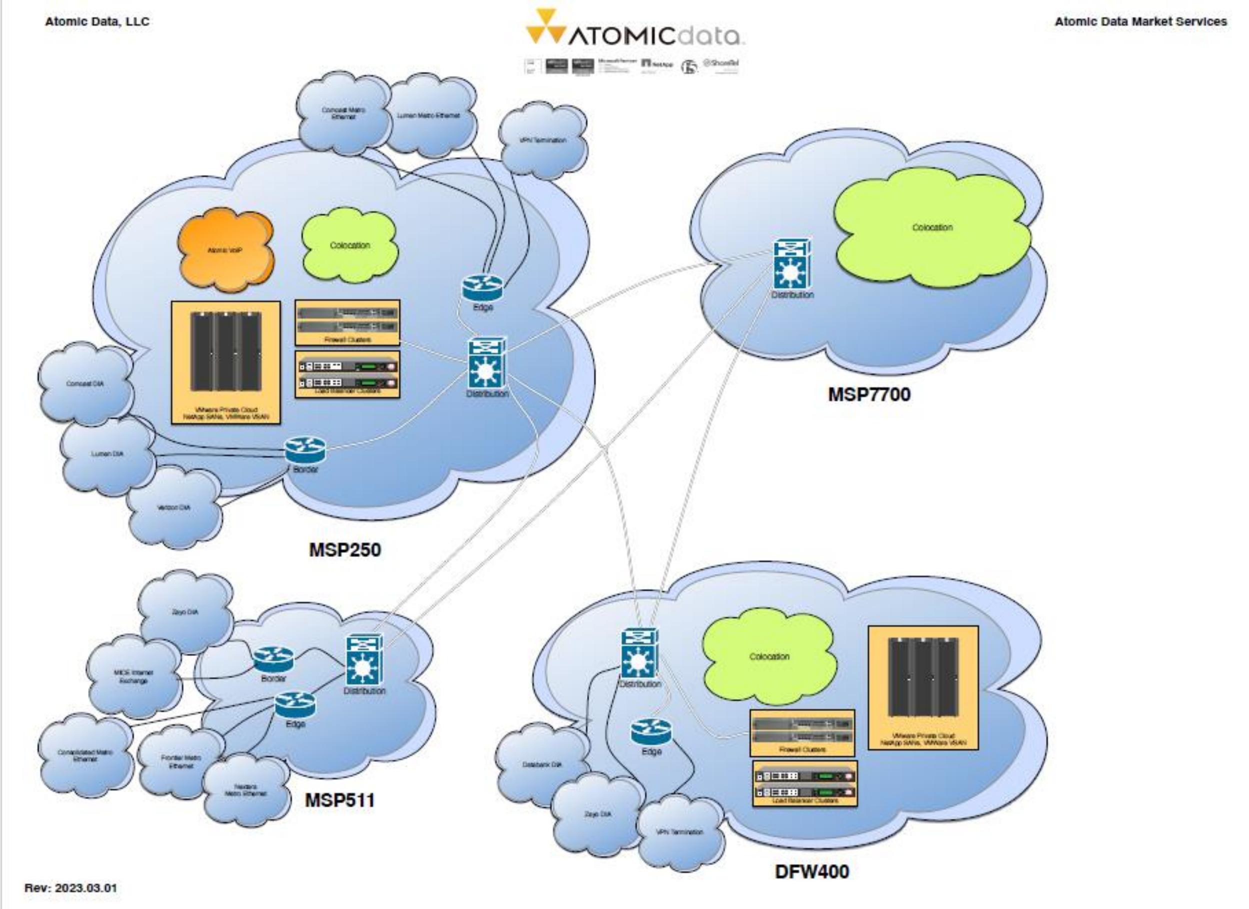
Client data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in client contracts.

Boundaries of the System

The scope of this report includes the Managed Services System products and services provided by Atomic Data in the two Minneapolis, Minnesota facilities and the Dallas, Texas facility.

This report does not include the colocation, environmental infrastructure, and preventative maintenance services provided by DataBank at the Edina, Minnesota and Dallas, Texas facilities, or the telecommunications services provided by Cologix at the Minneapolis, Minnesota facility.

Atomic Data Network Overview:



Changes to the System Since the Last Review

No significant changes have occurred to the services provided to clients since the organization's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to clients since the organization's last review.

Criteria Not Applicable to the System

All Common Criteria/Security, Availability, and Confidentiality criterion were applicable to the Atomic Data Managed Services System products and services.

Subservice Organizations

As noted above in the section on the Components of the System, Atomic Data operates within the following provider managed data center facilities:

- MSP511 - Operated by Cologix
- MSP7700 - Operated by Databank
- DFW400 - Operated by Databank

Subservice Description of Services

MSP7700 and DFW400 Data Center Infrastructure - DataBank

DataBank is a provider of data center infrastructure, communications, and related services, whose business offerings include secure, reliable space and high-speed dedicated and internet-based communications for primary and backup data facilities, hosting, or remote storage. DataBank operates multiple 24x7x365 commercial data centers throughout the United States. DataBank provides infrastructure protection to their clients via environmental monitoring and failover capabilities. DataBank also provides 24-hour availability of its personnel to respond to client inquiries.

DataBank offers carrier-class facilities designed to meet industry standards. Multiple high-speed fiber entrances into their facilities and redundant cooling and power systems are standard. Support services and equipment are available on an "as needed" basis allowing clients to outsource only the services they really need.

Atomic Data utilizes DataBank as a colocation and infrastructure service provider for the MSP7700 and DFW400 data center facilities. Both buildings are home to dozens of major network carriers, who support a common, secure perimeter for the entire facility and demand the highest reliability for common utility services.

Atomic Data occupies dedicated cages at these facilities, extending its standard access control, environmental monitoring, and video surveillance infrastructures to facilitate products and services. Clients may choose from rack, multi-rack, and dedicated cage colocation solutions. Atomic Data's network services include flexible switching, multi-homed dedicated internet, and point-to-point access to transport facilities via high-capacity metropolitan and long-haul network facilities.

MSP7700 Data Center

Network and Connectivity

- Diverse and secure telecom entries
- Diverse and secure fiber entries
- Multiple DataBank-controlled MMRs (Meet-Me-Room)

Heating, Ventilation and Air Conditioning (HVAC) and Environmental Design

- Redundant HVAC design for stable airflow, temperature, and humidity
- Highly efficient perimeter cooling system
- Hot-aisle/cold-aisle configuration
- Anti-static raised flooring and overhead cable runs allow unobstructed cold air delivery

Power

- 5MW of on-site power deployed via underground diverse delivery
- Dedicated parallel uninterruptible power supply (UPS) configuration
- Dedicated diesel generators
- Dedicated on-site fuel supply for each generator
- Fully redundant programmable logic controller (PLC) switching configuration
- Multiple redundant power distribution paths
- Branch circuit monitoring

Physical Security

- On-site security personnel 24x7x365
- Monitored security cameras and intercom system
- Fully secured mechanical/electrical equipment
- Dual-factor authentication (key card access w/secondary biometric) on exterior entry and data center halls

- Camera surveillance on ingress/egress points and critical areas
- Video with access log retention for 90 days
- Custom physical security controls available for customer deployments
- Power delivery, generator and diesel fuel infrastructure maintained in secured areas

DFW400 Data Center

Network and Connectivity

- Diverse and secure telecom entries
- Diverse and secure fiber entries
- Multiple DataBank-controlled MMRs (Meet-Me-Room)

HVAC and Environmental Design

- Redundant HVAC design for stable airflow, temperature, and humidity control
- Highly efficient perimeter cooling system
- On-site secured water storage tanks
- Hot-aisle/cold-aisle configuration
- Anti-static raised flooring and overhead cable runs allow unobstructed cold air delivery

Power

- 28.8MW (14.4MW A + 14.4MW B) of on-site power deployed via underground diverse delivery in a 2N design
- Dedicated 2N (A/B) UPS configuration
- Dedicated 2N (A/B) configuration for diesel generators
- Dedicated on-site fuel supply for each generator
- Fully redundant (2N) Automatic Transfer Switch
- (ATS) configuration
- Multiple redundant power distribution paths
- Branch circuit monitoring

Physical Security

- On-site security and support personnel 24x7x365
- Monitored security cameras and intercom system
- Full perimeter fence with secured parking
- Mechanical/electrical equipment are fully secured
- Dual-factor authentication (key card and secondary biometric) on data center entrances
- Camera surveillance on ingress/egress points and critical areas
- Video with access log retention for 90 days
- Custom physical security controls available for customer deployments
- Power delivery, generator and diesel fuel infrastructure maintained in secured areas

This report does not include the Colocation, Environmental Infrastructure, and Preventative Maintenance Services provided by DataBank at the Edina, Minnesota and Dallas, Texas facilities.

MSP511 Data Center Infrastructure - Cologix

Atomic Data utilizes Cologix as a network service provider at the MSP511 data center facility. Cologix is located within the 511 Building, the most highly connected telecommunications facility in Minnesota. The 511 Building is home to dozens of major network carriers who support a common, secure perimeter for the entire facility and demand the highest reliability for common utility services.

Cologix is a major provider within the building, providing telecommunications interconnect services for numerous ISPs and large entities. The building provides a secure entrance that is staffed 24x7 and monitored by security cameras. Cologix provides security at the suite, room, and rack level, ensuring no unauthorized access is permitted. Cologix also provides infrastructure protection to their clients via environmental monitoring and failover capabilities. Cologix also is available 24x7 to respond to client inquiries.

Atomic Data uses MSP511 to enhance services already available in the MSP market and add network redundancy. Multiple connections to major internet backbone providers and regional ISPs further enhance the availability of Atomic Data's IP transit services and reduce overall network latency. Atomic Data also uses MSP511 to provide enhanced local and long-haul point-to-point connectivity options for customers, allowing additional flexibility and more competitive pricing. Atomic Data does not store data or provide other services from this facility.

Complementary Subservice Organization Controls

The following subservice organization controls should be implemented by DataBank to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization Controls - DataBank		
Category	**Criteria**	**Applicable Controls**
Availability	A1.2	Data center areas are equipped with fire detection and suppression systems including: • Smoke detectors • Audible and visual fire alarms • Automated extinguisher system • Hand-held fire extinguishers
		Data center areas are equipped with multiple dedicated air handling units.
		On an annual basis, management contracts third-party vendors to complete inspections on the air handling units. Inspections and maintenance of air handling units is completed by licensed third-party vendors on a schedule equal or better to manufacturer recommendations.
		Data center areas are equipped with water detection devices to detect and mitigate the risk of water damage in the event of a flood or water leak.
		Data center areas are available with raised flooring and/or server racks to elevate equipment and help facilitate cooling.
		Data center power systems are constructed with redundant UPS units.
		UPS systems are equipped with maintenance bypass or "wrap around" breakers and can be isolated from the protected load during UPS maintenance.
		The data centers have redundant electrical utility feeds.
		Power infrastructure is designed and constructed redundantly to mitigate risk to customer systems and services.
		DataBank maintains policy and procedure manuals for backup, storage, and restoration procedures.

Subservice Organization Controls - DataBank		
Category	**Criteria**	**Applicable Controls**
		DataBank standard backup configuration is set to automatically perform daily backups of customer systems.
		An incident ticketing system is utilized to document, prioritize, escalate, and help resolve problems affecting services provided.

Atomic Data provides additional levels of monitoring and control independent of DataBank. A separate access control system is used to restrict access to the Atomic Data controlled cages. This system requires personnel to use proximity cards and PINs to access the cages. Access attempts are electronically recorded for future auditing and review. Digital surveillance cameras are operated by Atomic Data within its cages. These cameras are monitored 24x7 by the Atomic Data NSOC and camera footage is retained for a minimum of 90 days. The NSOC also monitors temperature and humidity in multiple areas, and historical data is retained for 365 days.

The following subservice organization controls should be implemented by Cologix to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization Controls - Cologix		
Category	**Criteria**	**Applicable Controls**
Common Criteria/Security	CC6.4	Visitors are required to register in a visitor log prior to accessing the data center facilities. Logs are reviewed on a monthly basis to ensure that the logs were filled out completely, and logs are retained at least 90 days.
		Employee/contractor access to the data center requires approval by the employee/contractor’s immediate entity supervisor.
		A badge access system is utilized to secure exterior and interior access to the office facility.
		The badge access system logs access attempts traceable to specific badge access cards. Security personnel review the access log on an ad hoc basis.
		Digital surveillance cameras are in place to monitor and record activity throughout the data center.
		Data centers are equipped with video surveillance cameras located throughout the premises and footage is retained for a minimum of 90 days.
		Badge access lists are reviewed monthly to help ensure data center access remains limited to authorized employee and customer personnel.
Availability	A1.2	A disaster recovery plan is maintained, updated, audited, and designed to respond to a range of facilities and/or operational incidents on a 24/7 basis that are a result of noncompliance with security policies.

Subservice Organization Controls - Cologix		
Category	**Criteria**	**Applicable Controls**
		Management performs an assessment to identify potential threats of disruption to systems including an assessment of the physical and environmental risks to the facilities.
		Uninterruptible Power Supply (UPS) systems are in place to provide backup power in the event of a power outage.
		Generators are located on the premises to provide backup power in under a minute in the event of power failure.
		Data centers are equipped with pre-action sprinkler fire suppression systems.
		Hand-held fire extinguishers are inspected annually.
		Environmental monitoring applications are utilized to monitor the environmental conditions within the data center and customer areas that include, but are not limited to, the following: • Temperature • Humidity and air quality • Power supply and voltage
		The environmental monitoring applications are configured to alert facilities and NOC personnel via e-mail alert notifications when predefined thresholds are exceeded.
		Air conditioning units are inspected on a quarterly basis.
		Generators are inspected and tested at least annually for proper performance in the event of a utility failure. Generator preventative maintenance is performed annually and tested under load conditions to help ensure proper operation during extended outages.
		UPS systems and batteries are inspected, and preventative maintenance is performed on at least an annual basis.
		Fire detection and suppression systems are inspected on an annual basis.

COMPLEMENTARY USER ENTITY CONTROLS

Atomic Data’s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. Atomic Data control procedures cannot feasibly solely achieve all the Trust Services Criteria related to Atomic Data’s services. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Atomic Data.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

Most Relevant Criteria Description	**User Entity Control Considerations**
CC6.1 CC6.6 CC6.7 CC6.8 CC8.1	Managed Firewall: Defining security policies and access lists appropriate for its environment.
CC6.7 CC6.8 CC8.1	Managed Virtual Server Guest Data Protection: Configuring its environment to effect specific backup policies at the operating system and application levels that exceed what the product provides, including requirements to meet greater granularity, frequency, or availability needs.
CC6.1 CC6.6 CC6.7 CC6.8	Remote Access Methods: Determining the appropriate level of network exposure and ensuring that individual accounts and services in the environment are properly managed and secured.
CC1.4 CC2.1 CC2.3	Acceptable Use of Network Services: Ensuring continuing, good-faith compliance with the Atomic Data Acceptable Use Policy.
CC6.1 CC6.2 CC6.4	Physical Colocation-Physical Access: Sending timely written notification from authorized users to Atomic Data of employee changes for physical access.
CC6.1 CC6.2 CC6.4	Physical Colocation-Network Security: Providing network security services for its equipment for which Atomic Data provides network access.
CC8.1	Operating System Security: Maintaining appropriate operating system patches, as well as determining the appropriate security standards for user accounts and restrictions on external administrative access, for customer servers running at Atomic Data.
CC6.1 CC6.2 CC6.3 CC6.7 CC6.8	Application Security: Maintaining the appropriate security standards for user accounts and maintaining restrictions on external administrative access for customer servers running at Atomic Data.
CC2.2 CC6.1	Autotask-Logical Access Administration: Sending timely written notification from authorized users to Atomic Data of employee changes for logical access administration. The customer is responsible for changing ticket and contact portal access passwords as well as administering users' privileges.

Most Relevant Criteria Description	User Entity Control Considerations
	Autotask-Administrative Security: Keeping the list of active contacts, authorization levels, and contact information up to date in the Contact Portal. When necessary, the customer must send timely updates of contact information and access levels.
	Autotask-Notification Groups: Notifying Atomic Data in a timely manner when maintenance notification groups should be updated to reflect changed personnel information.
A1.1	Connectivity Services-Customer Premises Equipment: Providing security, backup, and operational capacity customer for any customer-owned network devices that terminate Atomic Data Connectivity Services.
CC2.2 CC2.3	Software Security Requirements: Providing Atomic Data with prescriptive lists of security requirements necessary to protect the application.
CC6.7 CC8.1	Software Vulnerabilities: Identifying and remediating vulnerabilities within applications hosted at Atomic Data, which may include regularly patching content management frameworks to prevent misuse.

SECTION 4

OTHER INFORMATION
PROVIDED BY THE SERVICE ORGANIZATION

ATOMIC DATA ANNOUNCEMENT REGARDING INTERIM LEADERSHIP MOVES

May 8, 2023 - In the aftermath of Jim Wolford's untimely death, Atomic Data is announcing the following interim leadership moves:

Co-owner, co-founder, and former CTO Larry Patterson has stepped into the new role of Interim President. Having served as Atomic Data's CTO for over 20 years, Larry brings exceptional technical skill and organizational knowledge to the position. Larry continues to work alongside co-owner Dr. John Dowdle in providing broad organizational oversight and consultation to the company.

Dwayne Sapp, previously Director of Network & Security Operations Center, Client Support, Professional Services, and Client Security & Compliance has been appointed as General Manager. Dwayne has been an Atomic Data pillar since 2012 and brings not only a deep relationship with Jim Wolford but also vast organizational knowledge, operational excellence, and client focus to the newly created position. Mr. Sapp commented, "Jim was a friend and leader of epic proportions. He expected the best so he could give his clients the best. That philosophy drove us in 2001, it drove us last week, and it will drive us going forward. As Jim would say often, 'Now go take care of the clients!'".

The 200+ strong Atomic Data family is committed to honoring Jim's legacy in the best way we know how; by serving our clients.

We thank the community for the outpouring of love and support during this difficult time.

-The Atomic Data Family