Flexential

2019 FISMA High SECURITY ASSESSMENT REPORT (SAR)

Version 1.2

Version November 8, 2019

Flexential FISMA High SAR

Version 1.2 November 8, 2019

Prepared by

Identification of Organization that Prepared this Document		
A-LIGN	**Organization Name**	A-LIGN Compliance and Security, Inc (“A-LIGN”)
	Street Address	Rivergate Tower, 400 Ashley Drive
	Suite/Room/Building	Suite 1325
	City, State Zip	Tampa, FL 33602

Prepared for

Identification of IT Services Provider		
FLEXENTIAL	**Organization Name**	Flexential
	Street Address	8809 Lenox Pointe Drive
	Suite/Room/Building	Suite G
	City, State ZIP	Charlotte, NC 28273

Revision History

Date	Description	Version of SAR	Author
10/21/2019	Initial Draft SAR creation.	1.0	A-LIGN
10/25/2019	Final SAR with edits	1.1	A-LIGN
11/18/2019	Final SAR with additional edits	1.2	A-LIGN

TABLE OF CONTENTS

SECTION 1 - EXECUTIVE SUMMARY

1. INTRODUCTION

1.1 Security Assessment Report Overview

The purpose of the Security Assessment Report ("SAR") is to evaluate the information system against the security control baselines as defined in Federal guidelines, Flexential's policies and procedures and determine if there are any gaps or vulnerabilities. Testing activities were performed in accordance with the National Institute of Standards and Technology Special Publication ("NIST SP") 800-53A Rev. 4, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, dated December 2014. Each security control requirement is tested and found to be "Satisfied", "Other than Satisfied", or "Not Applicable". Gaps and vulnerabilities cause result of "Other than Satisfied", and if this is the case, recommendations are provided to assist Flexential in remediation.

The SAR is to be used at the discretion of Flexential. Examples of use include: for internal use only, and/or distribution to Agency or Client as requested.

The Federal Information Security Management Act of 2002 & Federal Information Security Modernization Act of 2014 ("FISMA") were enacted by the United States Federal government to mandate that federal agencies document and implement information security programs to protect their information systems and assets. As part of the Act, NIST was required to develop standards and guidelines in order to assist federal agencies implement their information security programs. As a result, NIST 800-53 is used a baseline to assess the information security program for FISMA.

1.2 System Information

Flexential was founded in 2017 through the combination of ViaWest Inc. (originally founded in 1999 and headquartered in Denver, Colorado) and Peak 10 (originally founded in 2000 and headquartered in Charlotte, North Carolina). Flexential currently employs approximately 1,000 employees across the United States. Flexential is headquartered in Charlotte, North Carolina. Flexential's executive management team consists of industry leaders with extensive experience in IT services and data center operations.

A variety of customized products are offered by Flexential, from strictly data center colocation through fully managed cloud environments. Colocation services include white floor space with dedicated and secure cabinets and cages, redundant power and critical infrastructure (UPS, cooling, fire prevention), physical security, and network connectivity / redundant telecommunication and bandwidth services.

Flexential provides colocation services in 20 geographic markets, across locations within the United States. With 40 physical data center locations and growing, Flexential operates raised floor gross square footage of well over 1 million square feet. Technical assistance and operational staff provide monitoring and customer support 24x7x365. Flexential's data centers reside in the following locations.

Data Center	Address
Allentown	744 Robel Road, Allentown, PA 18109
Atlanta - Alpharetta	12655 Edison Dr., Alpharetta, GA 30005
Atlanta - Norcross	2775 Northwoods Pkwy, Norcross, GA 30071
Austin	205 W 9th St, Ste 201, Austin, TX 78701
Charlotte - North	10105 David Taylor Dr., Charlotte, NC 28262

Data Center	Address
Charlotte - South	8910 Lenox Pointe Dr, Ste A, G, Charlotte, NC 28273
Cincinnati	5307 Muhlhauser Rd, West Chester Township, OH 45011
Dallas - Downtown	1950 N Stemmons Fwy, Dallas, TX 75207
Dallas - Plano	3500 E Plano Pkwy, Plano, TX 75074
Dallas - Richardson	3010 Waterview Pkwy, Richardson, TX 75080
Denver - Aurora	11900 E Cornell Ave, Ste A, Aurora, CO 80014
Denver - Centennial	12500 E Arapahoe Rd, Ste C, Englewood, CO 80112
Denver - Downtown	1500 Champa St, Ste 100, Denver, CO 80202
Denver - Englewood	8636 South Peoria St, Englewood, CO 80112
Denver - LoDo	501 Wazee St, Denver, CO 80204
Fort Lauderdale	5301 NW 33rd Ave, Fort Lauderdale, FL 33309
Jacksonville	4905 Belfort Rd, Ste 145, Jacksonville, FL 32256
Las Vegas - Downtown	302 Carson Ave, Ste 100, Las Vegas, NV 89101
Las Vegas - Downtown	304 Carson Ave, Las Vegas, NV 89101
Las Vegas - North	3330 E Lone Mountain Rd, North Las Vegas, NV 89081
Louisville - Downtown	752 Barret Ave, Louisville, KY 40204
Louisville - East	2101 Nelson Miller Pkwy, Louisville, KY 40223
Minneapolis - Chaska	3500 Lyman Blvd, Chaska, MN 55318
Nashville - Brentwood	7100 Commerce Way, Brentwood, TN 37027
Nashville - Cool Springs	425 Duke Dr, Ste 400, Franklin, TN 37067
Nashville - Franklin	4600 Carothers Pkwy, Franklin, TN 37067
Philadelphia - Collegeville	101 Troutman Rd, Collegeville, PA 19426
Phoenix - Deer Valley	1850 W. Deer Valley Rd, Phoenix, AZ 85027
Portland - Hillsboro 1	3935 NW Aloclek Pl, Bldg C, Hillsboro, OR 97124
Portland - Hillsboro 2	5737 NE Huffman Street, Hillsboro OR 97124
Raleigh	5150 McCrimmon Parkway, Morrisville, NC 27560
Richmond	8851 Park Central Dr, Richmond, VA 23227

Data Center	Address
Salt Lake City - Cottonwood	6340 S 3000 E, Ste 150, Salt Lake City, UT 84121
Salt Lake City - Downtown	572 Delong St, Ste 100, Salt Lake City, UT 84104
Salt Lake City - Fair Park	118 S 1000 W, Salt Lake City, UT 84104
Salt Lake City - Lindon	333 S 520 W, Lindon, UT 84042
Salt Lake City - Millcreek	3949 S 200 E, Murray, UT 84107
Salt Lake City - South Valley	7202 S Campus View Dr, West Jordan, UT 84084
Tampa - North	8350 Parkedge Dr., Tampa, FL, 33637
Tampa - West	9417 Corporate Lake Dr, Tampa, FL 33634

This SAR is evaluating the security controls around the Flexential data centers. Based on A-LIGN’s understanding of Flexential’s control environment, the information system is categorized as FISMA High based on the Federal Information Processing Standards Publications (“FIPS PUBS”) 199 Standards for Security Categorization of Federal Information and Information Systems. As such the assessment procedures performed by A-LIGN were for a FISMA High information system.

1.3 Scope

The scope of the assessment included Flexential's physical and environmental protection security controls implemented within data center facilities used by its customers for colocation services ranging across multiple industries to house their information systems and network components. Flexential directs their data center colocation services from their headquarters in Charlotte, North Carolina, where they managed all controls. The following twelve (12) data centers were selected as a sample for testing in this report:

Data Center	Address
1. Charlotte - North	10105 David Taylor Dr., Charlotte, NC 28262
2. Charlotte - South	8910 Lenox Pointe Dr, Ste A, G, Charlotte, NC 28273
3. Dallas - Plano	3500 E Plano Pkwy, Plano, TX 75074
4. Dallas - Richardson	3010 Waterview Pkwy, Richardson, TX 75080
5. Dallas - Downtown	1950 N Stemmons Fwy, Dallas, TX 75207
6. Austin	205 W 9th St, Ste 201, Austin, TX 78701
7. Las Vegas - Downtown	302 Carson Ave, Ste 100, Las Vegas, NV 89101
8. Las Vegas - Downtown	304 Carson Ave, Las Vegas, NV 89101
9. Las Vegas - North	3330 E Lone Mountain Rd, North Las Vegas, NV 89081
10. Portland - Hillsboro 1	3935 NW Aloclek Pl, Bldg C, Hillsboro, OR 97124
11. Portland - Hillsboro 2	5737 NE Huffman Street, Hillsboro OR 97124
12. Phoenix - Deer Valley	1850 W. Deer Valley Rd, Phoenix, AZ 85027

A selection of NIST Special Publication 800-53 revision 4 security controls were used as the basis for this assessment. The Physical and Environmental control family selection was agreed upon and requested by Flexential. The security controls define the policies and procedures, as well as the controls, that an organization should have in place to be compliant with FISMA.

The NIST 800-53 revision 4 control areas included in the assessment were the Physical and Environmental Protection controls.

Flexential Security Control Status Summary
(Total Controls: High (26))

ID	Control Description	Sensitivity Level
		High
PE	**Physical and Environmental Protection**	
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1
PE-2	Physical Access Authorizations	PE-2
PE-3	Physical Access Control	PE-3 (1)
PE-4	Access Control for Transmission Medium	PE-4
PE-5	Access Control for Output Devices	PE-5
PE-6	Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment	PE-6 (1) (4)
PE-8	Visitor Access Records	PE-8 (1)
PE-9	Power Equipment and Cabling	PE-9
PE-10	Emergency Shutoff	PE-10
PE-11	Emergency Power	PE-11 (1)
PE-12	Emergency Lighting	PE-12
PE-13	Fire Protection	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14
PE-15	Water Damage Protection	PE-15 (1)
PE-16	Delivery and Removal	PE-16
PE-17	Alternate Work Site	PE-17
PE-18	Location of Information System Components	PE-18

1.4 Security Assessment Methodology

A-LIGN submitted an information request list to the organization which requested evidence to demonstrate the implementation of the NIST 800-53 revision 4 security baseline controls. David Wong, Staff Consultant performed testing procedures for A-LIGN from 8/27/2019 to 10/19/2019. Onsite inspections and procedures for the sample selection of data center facilities were performed by the below A-LIGN consultants during the week of 9/10.

Name	Title	Data Center Locations
Patrick Ibrahim	Senior Consultant	North Carolina (2) Oregon (2)
Monica Armour	Senior Consultant	Nevada Facilities (3) Arizona Facilities (1)
David Wong	Staff Consultant	North Carolina (2)
Jacob Balmaseda	Staff Consultant	Texas Facilities (4)

In order to determine the effectiveness of the security controls, A-LIGN had to perform various tests. A-LIGN performed testing procedures based on the scope and locations defined above to determine if the controls listed in Flexential ’s Security Assessment Plan (“SAP”) and defined by NIST 800-53 revision 4 were implemented and operating as required. Testing procedures followed the guidance provided in NIST 800-53A revision 4 as defined in the table below and included interviewing Flexential personnel, inspecting evidence such as Flexential policies and procedures and system security setting, observing Flexential personnel and selecting samples of Flexential system components to ensure the Flexential's controls are in place.

Each requirement was designated to be “Common/Inherited”, “System-Specific” or “Hybrid” based on guidance in NIST 800-53 revision 4. Definition of each one is detailed below in the table:

Method	Definition
Interview	The process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.
Examine	The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.
Test	The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.

Control Designation	Definition
Common/Inherited	Common/Inherited requirements are those that are either inherited from one or more information system or shared between several information systems.
System-Specific	System-Specific requirements are those that are specific to the information system that is being assessed.
Hybrid	Hybrid requirements are those that are a combination of Common/Inherited and System-Specific.

List of individuals interviewed during the assessment:

Name	Title	Department
David Kidd	Vice President, Governance, Risk and Compliance	Governance, Risk and Compliance
Kim Wright	IT Security & Compliance Analyst	Compliance
Rebecca Browne	IT Security & Compliance Analyst	Compliance
Donald Burns	IT Audit & Compliance Specialist	Compliance
Kim Snider	HR Coordinator	Talent Acquisition
Steven Dockery	HR Director	Employee Relations
Jacob Cram	Physical Security Specialist	Control & Security
James Knabel	Physical Security Specialist	Controls & Security

SECTION 2 - SECURITY ASSESSMENT REPORT

2.1 SERVICES DESCRIPTION

Flexential's colocation services provide its customers:

- Convenient data centers with 40 nationwide
- Industry-leading compliance and standards
- Advanced security protocols
- Global interconnection capabilities
- Guaranteed uptime, built-in redundancies, professionals onsite 24/7
- Solutions that scale to meet changing business requirements
- Optional managed colocation services
- The Flexential team of hardware, software and hybrid IT professionals

Flexential's colocation services include white floor space with dedicated and secure cabinets and cages, redundant power and critical infrastructure (UPS, cooling, fire detection and prevention), physical security, and network connectivity / redundant telecommunication and bandwidth services. Specifically, the following are provided:

- Racks / Caging space
- Main electrical power
- Backup electrical power
- Environmental conditioning
- Fire detection and extinguishing systems
- Access and security control systems

Colocation services are available in 20 geographic markets, across locations within the United States. With 40 physical data center locations and growing, Flexential operates raised floor gross square footage of well over 1 million square feet. Technical assistance and operational staff provide monitoring and customer support 24x7x365.

Physical Security

General Physical Security

Flexential data center and facility support personnel are responsible for physical security and coordinated with the Flexential security team and senior management. Monitoring of physical security at each data centers is performed by local facilities personnel 24x7x365. Physical access protection at the data centers include a combination of physical access devices, such as keys, locks, combinations, biometric and card readers, mantraps, as well as security personnel to control entry to facilities.

Only authorized personnel who have been vetted or verified by Flexential and whose job function requires access to data centers are granted physical access to the data centers and to certain secured areas within them. These personnel include employees, customers or vendors. Only authorized visitors are allowed at the data centers and have very limited access.

<u>New or Modified Employee Physical Access</u>

All Flexential personnel are required to attend security training during the onboarding process and annually thereafter. Additional training in facilities operations, safety, and security is also required for staff in data center operational support roles. Physical access authorization for employees is documented in various forms or tickets and provisioned accordingly based on employees' role and responsibilities.

Vendor and Customer Access

Each customer must identify individuals (employees or third-party vendors) who are authorized to access Flexential's facilities. Customers have access to a customer portal, which is managed by a customer-designated administer, for managing individuals who are authorized to access facilities on the customer's behalf. Individuals can be granted permanent access or day pass only. The system generates a ticket for Flexential operations staff to process for each occurrence. The same process applies for revoking access. A badge is not automatically granted for vendors and customers after a request is submitted. Authorized individuals must physically show up at the designated data center, read and abide by Flexential's data center's rules, provide a valid government-issued picture ID, and sign an acknowledgement or accountability form, agreeing to the rules of the data center. Vendors are pre-authorized through the ticketing system and follow a similar process by presenting a valid ID and sign an acknowledgement/accountability form for first-time access and badge receipt.

Visitor Access

Visitors must check in at the security desk and be authenticated by operations personnel prior to being granted access to the data centers. Only authorized visitors on the data center's physical access list will be granted a visitors badge. Prior to being granted a badge, visitors must sign the visitor's access log to document the purpose of the visit and provide a valid government ID. Visitors' badges have no access to any doors and are clearly marked as 'Visitor'. All visitors must be escorted and monitored while at the facilities.

Facility Access Control

Flexential has implemented electronic key card systems at all of its data center facilities. Access lists govern which of the doors or the types of access an authorized individual has. Individuals who have been approved will be granted a valid access card for a specific data center and to secure areas based on their role and responsibilities. An individual must scan his or her card and provide personal PIN or biometrics associated with the badge in order to gain access to raised floor area or secure area(s). After an individual authenticates to the raised floor area, the individual must also have access to the customer's equipment through the use of another lock and key, badge, PIN, or biometric reader. Each customer is allocated his or her own space through the use of secured racks, cages, or suites. Access to sensitive areas such office area, technical assistance center, power room, and telecommunications room is restricted to authorized personnel only and is controlled by an access control system at each facility.

Customer Cage Access

The customer environments within each data center are physically secured within a locked cage, cabinet, or suite. Customer cabinets and cages are secured by keyed locks (keys secured via lock box), combination locks, card readers, biometric devices, and/or keypads per the customer's choice. Master keys are kept in a secure environment not accessible to customers or vendors. Onsite operational personnel are required to carry master keys, as well as data center managers and their direct reports (i.e., those who perform customer installations).

Shipping and Receiving Access

All parcels entering and leaving each data center are controlled, managed, and monitored by the local operational staff at each facility. Shipments are logged in shipping logs/tickets by Flexential and placed in a secured loading zones that are segregated from the rest of the data center until they are picked up or shipped. Couriers do not have access to the data center and must notify staff at the operations center of deliveries or pickups.

Physical Security Monitoring

Each Flexential data center has security cameras (CCTV) installed to monitor and record physical access events at key internal and external access points. This includes areas outside of the customer cages. Security cameras are motion activated and can record up to available memory capacity. Video feeds for key areas are retained for a minimum 90 days and may vary slightly between Flexential data center locations due to the amount of activity captured and storage capacity. Data center doors also have monitoring systems and alarms in place to alert facilities personnel if doors remain opened too long, are forced opened, or are opened when they should remain closed.

Facility personnel conduct monitoring of physical activity throughout each data center in the Operations Center. Some data centers also have security guards to monitor the data center premise. There are monitors that display activities from the security cameras in the Operations Center. Additionally, operations personnel perform facility rounds of each data center multiple times throughout the day to physically inspect each data center's building exterior, docks, storage facilities, security cameras, and security systems and to ensure that there are no physical access violations. Daily facilities rounds are documented and tracked in a ticketing system, as well as any physical security access violations or alerts during the monitoring process. Security incident tickets are opened for violations or issues that require further investigation.

Physical Security Access Reviews

Physical access reviews are performed at least annually to help ensure that only authorized employees have the correct physical access. Each data center has a physical access list of authorized individuals that is generated by a physical access control system. During the review process, the list is compared with current authorizations. Any exceptions noted are documented and tracked to resolution. Management also conducts logical access review of users with administrative access to the various physical access badging systems by comparing the current list of users against terminated employees. This ensures that the current access list is still valid and that users have the appropriate access for their job or roles. Exceptions are documented and sent to administrators of the respective systems for remediation. The access list is revalidated by management for accuracy and completion.

Visitor Access Records

Flexential also reviews access records regularly to ensure only authorized personnel can access the facilities. A ticketing system and reports from physical access control systems are used to assist with the review of visitor access records. Each data center facility maintains visitor access records for at least one year. Visitor access records include name of the person visiting, signature of the visitor, form of identification, date of access, time of entry and departure, purpose of visit, and name of person visited. Monthly review of these records are performed by local data operations personnel and the results are documented in tickets. There are also quarterly review of customer and Flexential employee access records as part of Flexential's internal quarterly audits. Discrepancies noted during the review process are documented and tracked using the ticketing system.

Environmental Security

General Environmental Security

Flexential data centers are equipped with environmental systems to help ensure that customer systems are available, protected, and monitored. UPS and generator systems provide redundant backup power at each data center to ensure that customer systems remain available and running. UPS' provide short-term power to support the entire data center until the generator is activated to provide long-term power. Flexential has agreements with third-party fuel providers to maintain sufficient fuel supply to avoid potential disruption in the event of long-term power outage. Emergency power shutoff help prevent electrical damage to equipment. There are HVAC systems at each facility to maintain temperature and humidity control. Each facility has a sufficient number of HVAC systems to allow for N+1 cooling redundancy on the raised floor. Critical infrastructure redundancy allows Flexential to perform scheduled maintenance and testing without impact customers and users. Fire and smoke prevention and detection systems, as well as fire extinguishers through the facilities, at each data center help protect against fire hazards. Fire detection and suppression systems are automatically activated in the event of a fire and notify operations personnel and local emergency responders. In addition to fire protection, each data center has water damage protection devices/systems such as drip pans, dry ropes, and a master shutoff valve to detect and/or prevent leaks or water damages to systems or computer equipment. Leak detection sensors under the raised flooring would trigger remote alarms notifying the facility personnel when a leak is detected.

To minimize any potential damages due to physical and environmental hazards, information system components are positioned away from the walls and are segmented from the rooms housing power equipment and cabling. There are hot and cool aisles to prevent computer damage. Power and communication cables are segregated. Cabling is located over or under the data center floors. Raised flooring helps mitigate information system components from water damage.

Environmental Security Monitoring

Data center personnel conduct site and environmental protection equipment inspections regularly to ensure that the facilities are compliant with Flexential's physical and environmental security standards. Flexential employs a building management system (BMS) in its data centers to monitor the status of key environmental systems, including power and cooling availability, temperature, humidity, and other elements. In addition to the BMS, operations personnel conduct visual inspection of environmental equipment. Finally, Flexential performs or contracts licensed vendors to perform routine preventative maintenance to mitigate any negative impact to its business operations and customer systems due to environmental issues. Inspections and preventative maintenances are logged and documented.

Daily Site Inspections

Daily facilities rounds are performed by data center personnel to inspect the facilities and verify that all critical systems and access security solutions are operational, and that environmental operating conditions remain within acceptable ranges. Any discrepancies or deviations are logged and documented in a ticket by a technician for remediation.

Generator Testing and Inspections

All generators are inspected annually as part of the preventative maintenance procedure. Start-up and run operation are conducted at least once per month and on-load testing is performed semi-annually or annually. Operating results are logged, and any issues are noted for follow-up and timely resolution.

Power Management and Semi-annual UPS Inspections

Power management equipment is in place at each data center for:

- A dedicated utility step-down transformer
- An automatic transfer switch that is connected to standby diesel generators

Mission-critical electrical loads at each data center are backed up by UPS systems. Semi-annual preventative maintenance procedures are performed on all UPS systems and batteries. Flexential also performs quarterly or annual inspections of all power distribution unit (PDU) systems. Any issues identified during the annual inspections are recorded for follow-up and resolved. Remote power panels (RPP) are used at some data centers instead of PDU and inspected every 6 hours. Both PDUs and RPPs are continuously monitored.

Fire Detection and Suppression Equipment and Inspections

Fire detection and suppression equipment are installed in all data centers. These include dry agent, overhead sprinklers, pre-action/double interlock dry pipe, laser, heat and smoke detectors, and VESDA. Semi-annual or annual fire inspection and annual preventative maintenance procedures are performed to confirm that the detection and suppression equipment is operating within optimal ranges.

HVAC Equipment

Each data center has an adequate supply of cooling capacity to support cooling requirements in the event of a loss of any critical cooling component. Computer room air conditioning units (CRAC) are used to monitor and maintain temperature and humidity levels. Preventative maintenance and vendor inspections are performed quarterly (every three months), at a minimum, on all cooling equipment. Building management systems (BMS) at each facility would alarm and notify data center operations personnel at the NOC and managers if humidity or temperature thresholds are out of range.

2.2 SECURITY ASSESSMENT RESULTS

The Security Assessment Results are summarized in the table below and the details of testing are documented in the matrices in Section 3. Each control is classified by two (2) parameters: Implementation Status and Assessment Result.

Implementation Status can be defined as:

- Implemented
- Partially Implemented
- Planned
- Alternative Implementation
- Not Applicable

Assessment Result can be defined as:

- Satisfied
- Other than Satisfied

A-LIGN identified no areas for improvement by Flexential.

SECTION 3 - TESTING MATRICIES

3.1 TEST CASE WORKBOOK

A-LIGN performed a FISMA High security control assessment for Flexential. Below is the test case workbook containing the assessment results derived from on-site testing and artifact examination for each security control.

Flexntial
FISMA_HIGH_SRTM.: