Notice

Limits on Report Access and Distribution

This document contains confidential and proprietary information and is to be treated as confidential. This report is intended solely for use by the management of Flexential Corp., its user entities (i.e., customers) that utilized the services covered by this report during the specified time period, and the independent financial statement auditors of those user entities (each referred to herein as a “specified user”).

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk.

Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.

When the useful life of this report is over, it must be destroyed.

FLEXENTIAL CORP.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

DATA CENTER AND CLOUD OPERATIONS SYSTEM

FOR THE PERIOD OF NOVEMBER 1, 2021, TO OCTOBER 31, 2022

Attestation and Compliance Services

INDEPENDENT SERVICE AUDITOR'S REPORT

To Flexential Corp.:

Scope

We have examined Flexential Corp.'s ("Flexential") accompanying assertion titled "Assertion of Flexential Corp Service Organization Management" ("assertion") that the controls within Flexential's Data Center and Cloud Operations system ("system") were effective throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that Flexential'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

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

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Flexential, to achieve Flexential's service commitments and system requirements based on the applicable trust services criteria. 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.

Service Organization's Responsibilities

Flexential 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 Flexential's service commitments and system requirements were achieved. Flexential has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Flexential is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve Flexential's service commitments and system requirements based on the applicable trust services criteria; and

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Flexential's service commitments and system requirements based on the applicable trust services criteria.

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

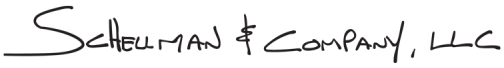
Inherent limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Flexential's Data Center and Cloud Operations system were effective throughout the period November 1, 2021, through October 31, 2022, to provide reasonable assurance that Flexential's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



Columbus, Ohio
November 13, 2022

ASSERTION OF FLEXENTIAL SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Flexential Corp.'s ("Flexential") Data Center and Cloud Operations system ("system") throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that Flexential's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below 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 November 1, 2021, to October 31, 2022, to provide reasonable assurance that Flexential'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Flexential's objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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

We assert that the controls within the system were effective throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that Flexential's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE DATA CENTER AND CLOUD OPERATIONS SYSTEM

Company Background

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 maintains headquarters in Charlotte, North Carolina and Denver, Colorado. The executive management team consists of industry leaders with experience in information technology (IT) services and data center operations.

Description of Services Provided

Flexential's colocation services is provided in 20 geographic markets, across locations within the United States. With 38 physical data center locations (Flexential managed) 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. Colocation services include white floor space with dedicated and secure cabinets and cages, redundant power, and critical infrastructure (uninterruptible power supply (UPS), cooling, fire prevention), physical security, and network connectivity / redundant telecommunication and bandwidth services. The company combines its nationwide data center footprint with its portfolio of cloud and managed services, to provide flexible hybrid IT services to customers throughout North America.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

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. Raleigh	5150 McCrimmon Parkway, Morrisville, NC 27560
4. Phoenix - Deer Valley	1850 W. Deer Valley Rd, Phoenix, AZ 85027
5. Denver - Aurora	11900 E Cornell Ave, Ste A, Aurora, CO 80014
6. Denver - Downtown	1500 Champa St, Ste 100, Denver, CO 80202
7. Denver - Centennial	12500 E Arapahoe Rd, Ste C, Centennial, CO 80112
8. Denver - Englewood	8636 South Peoria St, Englewood, CO 80112
9. Jacksonville	4905 Belfort Rd, Ste 145, Jacksonville, FL 32256
10. Fort Lauderdale	5301 NW 33rd Ave, Fort Lauderdale, FL 33309
11. Tampa - North	8350 Parkedge Dr., Tampa, FL, 33637
12. Tampa – West	9417 Corporate Lake Dr, Tampa, FL 33634
13. Atlanta - Alpharetta	12655 Edison Dr., Alpharetta, GA, 30022
14. Atlanta - Norcross	2775 Northwoods Pkwy, Norcross, GA 30071
15. Louisville - East	2101 Nelson Miller Pkwy, Louisville, KY 40223
16. Louisville - Downtown	752 Barret Ave, Louisville, KY 40204

Data Center	Address
17. Minneapolis - Chaska	3500 Lyman Blvd, Chaska, MN 55318
18. Las Vegas - Downtown	302 E. Carson Ave, Ste 100, Las Vegas, NV 89101
19. Las Vegas - Downtown	304 E. Carson Ave, Ste 370, Las Vegas, NV 89101
20. Las Vegas - North	3330 E Lone Mountain Rd, North Las Vegas, NV 89081
21. Cincinnati	5307 Muhlhauser Rd, West Chester Township, OH 45011
22. Portland - Hillsboro 1	3935 NW Aloclek Pl, Bldg. C, Hillsboro, OR 97124
23. Portland - Hillsboro 2	5737 NE Huffman Street, Hillsboro OR 97124
24. Allentown	744 Roble Road, Allentown, PA 18109
25. Collegeville	101 Troutman Rd., Collegeville, PA 19426
26. Nashville - Cool Springs	425 Duke Dr, Ste 400, Franklin, TN 37067
27. Nashville - Franklin	4600 Carothers Pkwy, Franklin, TN 37067
28. Nashville - Brentwood	7100 Commerce Way, Brentwood, TN 37027
29. Dallas - Downtown	1950 N Stemmons Fwy, Dallas, TX 75207
30. Dallas - Plano	3500 E Plano Pkwy, Plano, TX 75074
31. Dallas - Richardson	3010 Waterview Pkwy, Richardson, TX 75080
32. Salt Lake City - Cottonwood	6340 S 3000 E, Ste 150, Salt Lake City, UT 84121
33. Salt Lake City - South Valley	7202 S Campus View Dr, West Jordan, UT 84084
34. Salt Lake City - Lindon	333 S 520 W, Lindon, UT 84042
35. Salt Lake City - Millcreek	3949 S 200 E, Murray, UT 84107
36. Salt Lake City - Downtown	572 Delong St, Ste 100, Salt Lake City, UT 84104
37. Salt Lake City - Fair Park	118 S 1000 W, Salt Lake City, UT 84104
38. Richmond	8851 Park Central Dr, Richmond, VA 23227
39. Amsterdam (Equinix)	Luttenbergweg 4, 1101 EC Amsterdam NL
40. Seattle (The Westin Building)	2001 6th Avenue, Seattle, WA 98121

Principal Service Commitments and System Requirements

Flexential designs its processes and procedures related to Data Center and Cloud Operations system to meet its objectives for providing Data Center and Cloud Operations. Those objectives are based on the service commitments that Flexential makes to user entities, the laws and regulations that govern the provision of the Data Center and Cloud Operations system, and the financial, operational, and compliance requirements that Flexential has established for the services. The Data Center and Cloud Operations of Flexential are subject to the state privacy security laws and regulations in the jurisdictions in which Flexential operates.

Flexential's commitments regarding security, availability, and confidentiality are documented and communicated to internal and external users via policies and procedures and customer Service Level Agreements (SLAs). In addition, policies and procedures are communicated and acknowledged by the internal user community via company SharePoint.

Security, availability, and confidentiality commitments to user entities are documented and communicated in SLAs as well as in the description of the service offering provided online.

The principal security, availability and confidentiality commitments are standardized and include, but are not limited to, the following:

- The use of logical access controls to safeguard the storage of client data within the system boundaries;
- The maintenance of the information security program including Flexential's infrastructure, technical controls, processes, policies, and certifications;
- A comprehensive and flexible disaster recovery solution;
- 24x7x365 surveillance monitoring at data centers;
- The development, testing, and maintenance of business continuity plans for critical functions; and
- The retention and destruction of confidential data in accordance with Flexential's policies.

Flexential has also established system requirements that support the achievement of the principal service commitments. These requirements include the following:

- The use of encryption technologies to protect system user data both at rest and in transit;
- Role-based access control with the principal of least privilege;
- The use of firewalls to protect its network from the internet;
- System monitoring to detect inappropriate behavior on the network;
- Change management procedures to support the requisite authorization, documentation, testing, and approval of changes;
- Availability monitoring applications are in place to monitor the capacity and performance levels of systems supporting the services and alert operations personnel when predefined thresholds are exceeded; and
- Environmental monitoring systems equipped to monitor the environmental systems and conditions within the data centers.

Such requirements are communicated in Flexential's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired, trained, and managed. 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 the Data Center and Cloud Operations.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Badge card access system	Entrapass, Genetec, C-Cure	The badge card access system is utilized in conjunction with the biometric recognition access system to control access to the greater data center facilities and the raised floor within the datacenter facilities.
Biometric recognition access system	BioStar, BioConnect	The biometric recognition access system is utilized in conjunction with the badge card accesssystem to verify identity with two factor authentication prior to granting access to the datacenter facilities and the raised floor within the data center facilities.
Closed Circuit Television (CCTV)/Video	ExacqVision, Genetec	The CCTV system utilized in conjunction with the badge card access system to provide video coverage of entry/exit points and secure areas within the data center facility.
Firewalls	Fortigate FortiOS	Corporate firewalls are utilized to restrict trafficinto the management network, and service delivery firewalls are utilized to filter and route traffic for customer-specific environments.
Backup system	CommVault	Automated backup system software and network of servers that provide backup and recovery.
Routers and switches	Cisco NXOS	Routers and switches are utilized to route network traffic.
Virtual hypervisor	VMware vCenter	VMware vCenter server that provides authentication and restricts access to customer virtual environments.
VMware hosts	VMware (ESXi 6.0)	VMware ESX hosts for running customer virtualmachines.
Web portals	Embotics vCommander, Client Center, vCloud Director	Customer portal system, through which customers manage their virtual machines.

People

Flexential utilizes the following functional areas of operations to support the Data Center and Cloud Operations system:

- Executive management - responsible for organizing and overseeing activities, accomplishing goals, and overseeing objectives in an efficient and effective manner.
- Managed services - responsible for managing and protecting users' information and systems from unauthorized access and use while maintaining integrity and availability.

- Engineering - responsible for specifying, deploying, and maintaining infrastructure systems, security, and support for user entities.
- Professional services - responsible for providing user entities with assistance before and after the initial sale by providing information, guidance, delivering goods, and continued support.
- Marketing - responsible for marketing and sales functions.
- Operations - responsible for maintaining and operating data center infrastructure and user entities' information technology environments in an efficient manner through the use of staff, resources, facilities, and business solutions.

Procedures

Access, Authentication and Authorization

Formal IT policies and procedures exist that describe the logical access standard. Employees are expected to adhere to Flexential's policies and procedures that define how services should be delivered. These are located on the company's intranet and can be accessed by authorized personnel.

Access to network devices is controlled by the implementation of access control lists (ACLs) that limit where connections can be made from. Users authenticate to the network devices using Terminal Access Controller Access-Control System (TACACS+), which is administered via Cisco Access Control Server (ACS). ACS leverages Active Directory (AD) group membership to define permission levels in network devices, which are restricted by different group tier assignments. The user must also be defined to a specific group within TACACS+ in order to administer network devices. Authentication to TACACS+ is controlled through ACS. Access for a group tier is requested based on the necessity of the job function and must be approved by the employee's manager before access is granted. Rivest-Shamir-Adleman (RSA) SecurID two-factor authentication is also used for authentication to the network devices. Users have unique usernames and PINs in addition to the token. Authentication tokens change at a fixed interval of 30, 60, or 120 seconds. PINs are not required to change on any fixed schedule.

Administrative access to network devices is commensurate with job function and is limited to the engineering and operational support teams. In order to access the network devices, Flexential has created ACLs on each device to allow only certain internet protocol (IP) addresses to connect to the device.

Flexential has implemented logical security controls to restrict access to customer networks and data. When customers call or login online to request support services, Technical assistance center (TAC) personnel use a series of secret questions and answers to authenticate the user. The automated service management system is configured to store these customer-specific questions. Customer networks are secured through private virtual local area networks (VLANs) and firewalls on the Flexential managed services network.

Access to resources within the managed services environment is controlled via Windows Active Directory domain membership. To access customer servers, Flexential personnel are assigned access to Windows groups, which are then assigned rights on customer servers. To access customer network devices and firewalls, ACLs on each device restrict access to allow only certain IP addresses the ability to connect to the device. The user must also be defined to a specific AD group configured on the ACS tool in order to administer the network devices using Radius. These configurations are defined on each network device. Access to the Flexential customer portal uses multi-factor authentication and is granted via membership within the ticketing system, which for Flexential employees uses authentication via the Flexential managed services domain.

Each customer environment has its own VLAN segregated by IP address. Management network domain users are authenticated via a user account and password before being granted access to the network. Password parameters and lockout requirements are enforced through a group policy on the managed services network and the network is configured to enforce the following password and lockout requirements:

- Minimum password length
- Password age (minimum and maximum)
- Password history

- Password complexity requirements
- Account lockout duration
- Account lockout threshold
- Account lockout counter reset

Access Requests and Access Revocation

Employees have access to Flexential systems, applications, and network devices, with access-level restrictions based on specific job functions that the user performs for Flexential. New access to the network is initiated by the hiring manager. HR provides the hiring manager with the new employee setup form to fill out and submit to the technology services department and an onboarding ticket is generated. Access rights are assigned based on the function/role identified on the new employee setup form.

Requests for user access modifications is initiated by the employee's manager by submitting the employee role change form to the technology services department and a ticket is generated. Access rights are modified based on the function/role identified on the employee role change form.

The employee's manager initiates the employee termination process by alerting the HR department using the Learning Management System (LMS). HR then approves the termination which creates a parent ticket in the service management system for the Technology Services department to revoke the employee's logical access to the Flexential corporate domain. The HR department and/or the employee's manager conducts an exit interview with the terminated employee and collects Flexential assets. Child tickets are generated from the parent ticket that are assigned to relevant departments to revoke access from other Flexential facilities, network devices, and systems.

For managed services, customer servers utilize either a customer-managed domain or the managed services domain. Administrative access to servers on customer-managed domains is controlled by the customer and the customer is responsible for administering account access to Flexential.

Administrative access to servers managed on the Flexential managed services domain is controlled by Flexential, and access is restricted through domain group membership. Administrative access to Linux servers is controlled via Public Key Infrastructure, and keys are granted to a limited number of Linux engineers who require access to maintain the servers.

To help ensure that access to systems, applications, and network devices remains authorized over time, compliance personnel perform logical access reviews on users who have access to the corporate domain and network devices. This review consists of inspecting the entire user base to verify that no terminated employees have access to the systems and to verify that users' current access rights are still required based on job changes or roles they are currently fulfilling within the organization. Any exceptions identified by management are sent to the system administrators of the respective systems for resolution, and the changed access lists are revalidated for completion of the review by management.

New customer environments within the Flexential data center facilities are required to meet standards set by management. Those standards are based on mutually agreed upon criteria and contractual obligations. Provisioning policies and procedures are documented to guide the provisioning process in new customer implementation and maintenance activities that include, but are not limited to, the following:

- Developing a customer profile within Salesforce and project record within the service management system;
- Creating project tasks and milestones and assigning sub-tasks;
- Project management monitoring and completion task responsibilities; and
- Managing changes to customer implementation order.

Procedures for customer implementation tasks and resolution of issues are facilitated by the provisioning personnel. Standard build procedures are maintained to guide the customer implementation process. The build procedures include tasks for installation and maintenance of the following:

- Active Directory

- Server installation
- Domain setup
- Windows installation
- Certificates
- Virtual Private Networks (VPNs)
- Service applications

Physical Security

Physical security of the data centers is the responsibility of data center and facility support personnel, along with coordination with the security team and senior management. Physical access to Flexential locations is monitored by facilities personnel 24x7x365.

Flexential data center facilities employ physical security controls to help ensure that only authorized personnel access the data centers. Documented physical security policies and procedures are in place to guide personnel in physical security administration as well as vendor administration procedures. Each data center facility is equipped with two separate two-factor authentication systems to control access. A Flexential badge is required to enter the buildings while a badge and PIN code, or a badge and biometric fingerprint scan, are required to enter the data center rooms. After successful authentication into the data center raised floor area, there are additional physical security controls that are required to access the customer's equipment using another lock and key, badge, PIN, or biometric reader. Each customer is allocated their own space through the use of secured racks, cages, or suites.

Visitors are required to sign in at the front desk prior to entering Flexential facilities and must be accompanied and supervised by a Flexential employee or an authorized client escort. Visitors are also required to wear a visitor badge while in Flexential facilities at all times. Visitor badges do not allow unescorted access to the facility or data centers. TAC personnel are staffed at the data center facilities to log visitor access and monitor the digital surveillance systems at the data centers on a 24-hour basis.

Flexential data center facility physical access activity is monitored through various monitoring systems. Each Flexential data center facility has security cameras installed to monitor and record physical access events.

Data is recorded based on activity/motion with the minimum data retention period for certain areas of 90 days. Data center facility doors also have monitoring systems in place to alert facilities personnel regarding doors that remain open too long, doors that are forced open, or doors that are opened that should remain closed. Camera activity is fed to the TAC and monitored by facility personnel. Data center personnel at each data center perform facility rounds multiple times throughout the day to physically inspect each data center's building exterior, docks, storage facilities, security cameras, and security systems. This helps to ensure that physical security systems are operating as designed.

Change Management

Policies and procedures are in place to guide personnel in documenting, scheduling, and performing infrastructure changes and maintenance activities. Changes related to facility and environmental systems and IT infrastructure that are known to, or have the potential to, affect customer services are placed in a scheduled change window. Any change to Flexential systems or infrastructure, including additions, deletions, or modifications, are required to follow the change management guidelines.

Operations and support personnel utilize the service management system to centrally track infrastructure change requests and maintenance activities. Information security is a key factor in assessing risk. Flexential has configured the risk assessment matrix within the service management system to measure complexity and impact to conduct the risk evaluation process. The tool will require change records to undergo risk assessment before submission. Reviewers and approvers of proposed changes will consider the impact to Flexential's information security when assessing the potential risk of a change.

Infrastructure and maintenance activities are determined by the rated risk and listed type of the following change:

- Low risk and normal – low risk normal changes do not require a second level of review or approval.

- Low risk and expedited/emergency – expedited and emergency changes require a second level Change Advisory Board (CAB) approval by the change manager. The change manager may provide an ad hoc review or conduct a review in the weekly CAB session.
- Medium risk (normal/expedite/emergency) – medium risk changes (other than standard) always require a second level CAB approval by the change manager. The change manager may provide an ad-hoc review or conduct a review in the weekly CAB session.
- High risk (normal/expedite/emergency) – high risk changes (other than standard) always require a second level CAB approval. Where time allows the change manager will seek to conduct a review in the weekly CAB session, but work may need to be completed before this approval can be documented. The change manager may provide an ad-hoc review.
- Flexential-initiated (any risk rating) – Flexential-initiated change types do not require second level review. Instead, these change types require confirmation that the change event schedule has been approved by the impacted customer.

Routine activities are a list of operational changes that pose no risk of customer impact and are associated with day-to-day operations. Such activities do not require any change record, not even a standard change.

A CAB meets weekly to review and approve changes, and each change ticket is evaluated on a case-by-case basis for the desired scheduling timeframe. A standard change record only requires management review/approval if it encounters a conflict and needs a conflict-override. Changes will be implemented in accordance with the Methods of Procedure and Standard Operating Procedures (MOP/SOP) and will be documented in such a way as to provide affected parties with the information required to evaluate the impact/results of the change and to successfully carry out the assigned functions following the change. The ability to implement changes into the production environment is restricted to user accounts accessible by authorized personnel.

Data Backup and Disaster Recovery

As part of the Flexential managed service solutions, an automated backup system is available for subscribing customers. A default backup configuration is utilized to perform system backups (full weekly and daily incremental backups). The backup system status notifications are available for subscribing customers through the web portal. A backup restoration is performed as a component of the business operations.

Flexential has policies and procedures in place related to disaster recovery and the management of emergency situations. This plan is tested on an annual basis. An emergency is defined as: any unplanned event that causes or has the potential to cause deaths or significant injuries to employees, customers, or the public; or that can significantly disrupt operations, cause physical or environmental damage, or threaten Flexential's financial standing or public image. The term "disaster" is deliberately not used within Flexential's policies and procedures document to avoid confusion with large-scale natural events or the overwhelming image it portrays.

The incident command system (ICS) methodology is outlined for Flexential's employees for responding to emergency situations. Flexential uses the ICS approach to facilitate internal emergency management and to coordinate with outside authorities.

The ICS provides a structured approach to declaring an emergency, managing an emergency, managing central communications, and transitioning an emergency over to outside authorities. Under this approach, a single individual, the incident commander (IC) is the primary decision-making authority to mitigate and resolve an emergency situation. An emergency operations center (EOC) serves as the communications center to coordinate internal communications and manage information. The crisis management team (CMT) serves to provide a management team to direct specific activities in specific areas of expertise.

As it relates to technological emergencies, Flexential has outlined these to include any interruption or loss of utility service, power source, environmental control, information system or equipment needed to maintain Flexential's operations. Loss of power would have significant consequences for Flexential's operations; for that reason, facilities are designed with redundant power systems, including facility uninterruptible power supplies and generator systems. These systems are designed to provide continuous power in the event of a loss of utility power. In the event of a loss of utility power, the local critical incident manager (CIM) will be designated as the IC. The incident commander will take steps to ensure continued power to critical systems using available redundant systems.

Flexential's network infrastructure is critical to the operation of key systems as well as customer's systems. In the event of an interruption in network connectivity, the network manager shall be designated as the IC. The incident commander will coordinate efforts with carriers and customers to return normal communications as quickly as possible.

Environmental Security

Flexential has implemented and documented policies and procedures to ensure the environmental security of each data center. When a new data center is commissioned, management obtains a report from a third-party specialist to ascertain that each new data center has been properly commissioned. These reports include reviews of project specifications and submittals, inspections of equipment installations, observations of original equipment manufacturer (OEM) startups, and reviews of electrical and mechanical infrastructures.

Data centers are equipped with fire and smoke detectors which trigger visible and audible alarms in the event of a fire. Pre-action dry-pipe water sprinklers or agent-based fire suppression systems are present at each location along with hand-held fire extinguishers to allow for prompt suppression of fires. Management contracts with third-party specialists to inspect the fire detection and suppression systems on an annual basis and the inspection reports are retained as evidence of completion. Facilities personnel inspect the hand-held fire extinguishers on a monthly basis, while a third-party inspects the fire extinguishers on an annual basis. Documentation of each inspection is retained.

The data centers are equipped with multiple air conditioning units to regulate temperature and humidity. Management contracts with third-party specialists to inspect the air conditioning units on a quarterly basis and the inspection reports are retained as evidence of completion. The data centers are equipped with water detection devices to detect and mitigate water damage in the event of a flood or water leak. These water detection units are placed near the air conditioning units, either in drip pans or under the raised floor.

Each data center is equipped with fueled electric power generators and redundant UPS systems to provide continuous power in the event of an outage. The generators and UPS systems are each inspected for maintenance and load tests by a third-party on a quarterly basis. Management obtains reports for completed maintenance activities and inspections.

Environmental monitoring systems are utilized to monitor the environmental systems and conditions within the data centers including fire alarm status and suppression systems, temperature, humidity and air quality, power levels and availability. The environmental monitoring application is configured to notify operations personnel via on-screen or e-mail alert notifications if certain predefined thresholds are exceeded on monitored systems. Lastly, TAC personnel perform multiple daily patrols to monitor and record readings from certain environmental equipment.

Incident Response

Cloud, managed services, and network service levels are monitored by a dedicated governance, risk, and compliance (GRC) group to ensure compliance with organizational policies and customer requirements. In addition, facilities are monitored 24x7 by facilities engineers. Staff members are in place either on-site or on call after business hours to monitor and resolve problems affecting services provided.

Incident response and support procedures are in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting managed and network services and include the following:

- Severity level definitions;
- Escalation procedures; and
- Response time requirements for service alerts.

An automated service management / ticketing system is utilized to document, prioritize, escalate, and resolve problems affecting the services provided. The ticketing system is configured to include the incident date, time, summary, contact name, status, impact level, urgency, and associated SLA.

System Monitoring

Documented standard build procedures are utilized for the installation and maintenance of production systems. These build procedures help ensure a consistent configuration for production systems. An intrusion detection and prevention system (IDPS) are utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to send automated e-mail notifications to IT personnel when predefined thresholds are exceeded.

An enterprise monitoring portal is available for subscribing customers. The monitoring application is configured to alert operations personnel via onscreen and e-mail alert notifications when certain predefined thresholds are exceeded on monitored systems. Performance metric and service level reports including availability, alert history, and trend analysis are available. The enterprise monitoring application is utilized to monitor the following:

- Availability of the network, host services and ports;
- IP packet transmissions and latency;
- Bandwidth utilization and performance; and
- Central processing unit (CPU) and hard disk utilization.

To further ensure the security of the system, a central anti-virus software is utilized on production systems and are configured to perform scans of monitored systems and updated registered clients on real-time basis. The central anti-virus is also configured to perform weekly scans for any new files installed on monitored systems and all files received, downloaded, copied, or modified.

Penetration testing is conducted to measure the security posture of target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Flexential. The third-party vendor's approach begins with a vulnerability analysis of the target system. This is performed to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed on a quarterly basis in accordance with Flexential policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Flexential. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Data

User entities are responsible for the procedures, by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to them; additionally, user entities are responsible for the procedures and controls governing the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions processed within this environment; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for those user entities.

Requests for services are initiated and authorized by user entities by directly contacting the customer support department. Customer requests are recorded and tracked within an internal ticketing system through resolution. The ticketing system is utilized to document, prioritize, escalate, and resolve problems affecting contracted services. Customer requests are managed according to established SLAs.

Information Category	Description	Examples
Unclassified Public	Information is not confidential and can be made public without any implications for Flexential. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	· Product brochures widely distributed · Information widely available in the public domain, including publicly available Flexential web site areas · Downloads of Flexential documents and whitepapers provided for public consumption · Reports required by regulatory authorities · Information approved for public release
Proprietary	Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence Flexential's operational effectiveness, causes an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	· Passwords and information on corporate security procedures · Know-how used to process client information · Standard operating procedures and policies used in all parts of Flexential's businesses · Flexential-developed software code, whether used internally or sold to clients
Customer Confidential Data	Information received from customers in any form or processing in production by Flexential. The original copy of such information must not be changed in any way without written permission from the customer. The highest possible levels of integrity, confidentiality, and restricted availability are vital. Personal identifiable information (PII) and personal health information (PHI) entrusted to Flexential is considered 'confidential.' PII and PHI data owned by customers residing within Flexential compliant systems must be encrypted and maintained per contractual obligation. PII and PHI data owned by Flexential must be encrypted and maintained by Flexential per the information security policy. Access is restricted based on the individual's role and current responsibilities. Access will not be granted unless a legitimate business-oriented need for such information exists. Third parties supporting Flexential are required to maintain the same level of standards to ensure PII is protected.	· Customer media · Electronic transmissions from customers · Product information generated for the client by Flexential production activities as specified by the customer
Customer Hardware Assets	Hardware assets leased by the customers that reside within customer space. Assets should be considered sensitive/restricted as data that would not classify as PII or PHI may reside on assets but would still be considered sensitive/restricted. Hardware assets purchased by customers and installed in a Flexential facility, such as key management systems may also be classified as sensitive/restricted	· Customer leased servers, network switches, or firewalls · Customer purchased technologies such as key management systems, which are installed in Flexential facility

Information Category	Description	Examples
Flexential Confidential Data	Information collected and used by Flexential in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	· Salaries and other personal data · Accounting data and internal financial reports · Confidential customer business data and confidential contracts · Non-disclosure agreements with clients/vendors · Flexential business plans
Vendor/Partner Confidential	Information that can be disclosed to a vendor or partner who has signed non-disclosure agreement (NDA) agreement, e.g., standard master service agreement (MSA), however, the vendor/partner cannot share the information outside of their organization.	· Contracts · Vendor/partner facing documents · Non-sensitive · Client-specific information · Proprietary information
Third-Party Personally Identifiable Information	Third-party PII is data collected by Flexential's clients that can be used alone or with other sources available to identify a specific individual. This information is generally protected by one or more statutory or regulatory requirements such as HIPAA, PCI DSS, EU directive 95/46/EC, GDPR, as well as other state and federal consumer privacy protection laws. Access to this information is highly restricted and is generally unnecessary in the course of normal operations. The highest possible levels of integrity, confidentiality, and restricted availability are vital to conform to contractual, legal, and regulatory requirements Flexential should encrypt any third-party PII under its control during transmission and storage.	· Personally identifiable information includes: · Full name (if not common) · National identification number · IP address (in some cases) · Vehicle registration plate number · Driver's license number · Face, fingerprints, or handwriting · Credit card numbers · Digital identity · Birthday · Birthplace · Genetic Information
EU Personal Data	Any information relating to an identified or identifiable natural person (i.e., information that can identify a person AND non-identifying information that can be linked to an identifiable person) in the European Union. The person does not have to be a formal resident of the EU, but their personal data must relate to their presence in the EU (e.g., the collection of personal information from a US resident while traveling on business in the EU constitutes "EU personal data").	· A data subject in the EU's: · Name. · Financial account information. · Government identification number. · Location data. · Online identifier (e.g., internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags); or · Factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person

Subservice Organizations

The managed security monitoring services provided by BAE Systems, Inc. and data center colocation services provided by Equinix, Inc. (Equinix), and The Westin Building were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at BAE Systems, Equinix, and The Westin Building, alone or in combination with controls at Flexential, and the types of controls expected to be implemented at BAE Systems, Equinix, and The Westin Building to achieve Flexential's principal service commitments and system requirements based on the applicable trust services criteria.

Control Activities Expected to be Implemented by Subservice Organizations	Applicable Trust Services Criteria
BAE Systems is responsible for an intrusion detection system utilized to analyze network events and report possible or actual network security breaches.	CC6.1 CC6.6 CC6.7 CC7.1 CC7.2
BAE Systems is responsible for configuring the system to notify personnel upon intrusion detection.	
Equinix and The Westin Building are responsible for physical access control systems to restrict access to and within the corporate facility and data center housing the facilities, backup media, and other system components such as firewalls, routers, and servers to properly authorize individuals.	CC6.4
Equinix and The Westin Building are responsible for establishing and adhering to policies and procedures to ensure changes made to physical access privileges for customers is in accordance with standard operating procedure.	
Equinix and The Westin Building are responsible for reviewing visitors, customers, vendors, and contractors government issued ID prior to allowing access to the facilities.	
Equinix and The Westin Building are responsible for completing a termination form and remove physical access to the facilities as a component of the employee termination process.	
Equinix and The Westin Building are responsible for ensuring the following equipment is in place for each facility: · Fire detection and suppression · Power management	A1.2
Equinix and The Westin Building are responsible for performing scheduled maintenance procedures to ensure that: · Fire detection and suppression equipment is working properly · Test and confirm the operation of power maintenance systems · HVAC equipment, cooling equipment, and leak detection sensors are working properly	
Equinix and The Westin Building are responsible for maintaining and monitoring temperature and humidity throughout the facilities through the use of air conditioning and ventilation equipment.	
Equinix and The Westin Building are responsible for monitoring the facilities 24x7 and that staff members are in place either on site or on call 24x7 who are alerted by the building management system (BMS) for system exceptions.	
Equinix and The Westin Building are responsible for implementing emergency procedures to help guide personnel in protecting against disruptions caused by an unexpected event.	

Complementary Control Responsibilities at User Entities

Flexential's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

However, in order for user entities to benefit from the Data Center and Cloud Operations system and its controls, the following responsibilities should be considered by user entities:

#	Control Responsibilities to be Considered by User Entities	Related Applicable Trust Services Criteria
1.	User entities are responsible for ensuring that access control and authentication system of their infrastructure are operating effectively.	CC6.1 CC6.2
2.	User entities are responsible for ensuring that actual or attempted security breaches to their network(s) and infrastructure are monitored and detected.	CC6.1 CC6.6 CC6.8
3.	User entities are responsible for ensuring that firewall and system logging are enabled and sufficient for their purposes.	
4.	User entities are responsible for ensuring that users follow the physical access procedures outlined in the customer agreement for visits to all data centers, and ensuring their cabinets are locked and their equipment is secured prior to leaving the premises. User entities are responsible for maintaining their own system(s) of record.	CC6.4
5.	User entities are responsible for ensuring that timely response to known or suspected incidents reported by Flexential personnel.	CC7.2 CC7.3 CC7.4 CC7.5
6.	User entities are responsible for ensuring that the impact of scheduled maintenance activities to their production processes and jobs is sufficiently mitigated.	CC8.1
7.	User entities are responsible for ensuring that the notification or denial of requested infrastructure changes.	
8.	User entities are responsible for ensuring that testing and backup restorations is being performed.	A1.3

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the Data Center and Cloud Operations system.