OVH US LLC DBA OVHCLOUD

SOC 3 REPORT

FOR THE OVHCLOUD SERVICES SYSTEM

FOR THE PERIOD OF JANUARY 1, 2025, TO DECEMBER 31, 2025

Attestation and Compliance Services

INDEPENDENT SERVICE AUDITOR'S REPORT

To OVH US LLC dba OVHcloud:

Scope

We have examined OVH US LLC dba OVHcloud's ("OVHcloud" or the "service organization") accompanying assertion titled "Assertion of OVHcloud Service Organization Management" ("assertion") that the controls within the OVHcloud Services system ("system") were effective throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that OVHcloud'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).*

OVHcloud uses a subservice organization for data center hosting and application development 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 OVHcloud, to achieve OVHcloud'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 organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

OVHcloud 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 OVHcloud's service commitments and system requirements were achieved. OVHcloud has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, OVHcloud 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.

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

Our examination included the following:

- 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 OVHcloud's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve OVHcloud'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 OVHcloud'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 the OVHcloud Services system were effective throughout the period January 1, 2025, through December 31, 2025, to provide reasonable assurance that OVHcloud's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Schellman & Company, LLC

Chicago, Illinois
March 20, 2026

ASSERTION OF OVHCLOUD SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within the OVHcloud Services system ("system") throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that OVHcloud'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 January 1, 2025, to December 31, 2025, to provide reasonable assurance that OVHcloud'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)*. OVHcloud's objectives for the system in 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 January 1, 2025, to December 31, 2025, to provide reasonable assurance that OVHcloud's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE OVHCLOUD SERVICES SYSTEM

Company Background

OVH US LLC dba OVHcloud ("OVHcloud") is a subsidiary of OVH Group, a global cloud provider offering Dedicated Servers, VMware® based Hosted Private Cloud, and OpenStack-based Public Cloud to over 1.6 million customers worldwide. OVH Group manages 44 data centers spanning four continents with 100 Tbps global network capacity, 44 redundant Points of Presence (PoPs), and 33 Local Zones worldwide.

- OVHcloud is vertically integrated: OVHcloud builds their own data centers and servers, owns and operates their own network, and are responsible for the maintenance and support for their customers.
- OVHcloud has one of the lowest Power Usage Effectiveness (PUE) in the industry. Mainly due to OVHcloud's patented liquid cooling system runs cold water through a maze on the CPU which eliminates the need for conventional air conditioning.
- OVHcloud is a pure-play infrastructure provider that provides and maintains servers to ensure high availability, performance, and connectivity allowing customers to concentrate on building their business.

Description of Services Provided

OVHcloud is a cloud service provider offering scalable virtual, dedicated, or hybrid solutions for servers, containers, storage, and applications.

The OVHcloud system is supported by two strategically located Data Centers for customers who choose to have their infrastructure located in the United States: Vint Hill, Virginia (East Coast), and Hillsboro, Oregon (West Coast). These locations are equipped with redundant and scalable infrastructure and contribute to the expansion of OVH Group's global fiber network.

Service Options

The OVHcloud Services system includes the following five (5) service offerings:

- **Hosted Private Cloud (HPC)** provides a single tenant with dedicated computer servers, physically isolated for optimal performance and Anti-Distributed Denial of Service (DDoS) protection, dedicated storage volumes, and dedicated cloud management instance. Infrastructure capability may be allocated to a single virtual Data Center or to multiple Data Centers, at the customer's option.
- **Dedicated Servers (Bare Metal)** provide a single tenant with internal automation provision with more than 30 operating systems and licenses available for installation. Dedicated Servers include anti-DDoS protection to mitigate a customer's risk of attacks and help support system availability.
- **Public Cloud Instance (PCI)** provides multi-tenant virtualized logically isolated resources on shared physical infrastructure, configured as a single virtual data center with network resources. Public Cloud Instance includes Anti-DDoS protection to mitigate a customer's risk of attacks and help support system availability.
- **Virtual Private Servers (VPS)** provide a virtualized logically isolated server on shared physical infrastructure with internal automation provisions that allow more than 30 operating systems and licenses available for installation. VPS include Anti-DDoS protection to mitigate a customer's risk of attacks and help support system availability. VPS is a compromise between a Dedicated Server and a Public Cloud Instance.
- **Managed Kubernetes Service** simplifies the deployment, scaling, and management of Kubernetes clusters, including updates related to bug fixes and security patches allowing developers to focus on building and deploying their applications.

Service Objects

Each type of service includes the capability to access the following objects and manage them to align with different consumption and administration models:

- **Virtual Data Centers** in different types of services will be set up and managed with optional internal network, edge gateway, and storage. Customer vSphere instances are configured with network address translation (NAT) allowing them to access the network.
- **Physical Servers** in different configurations will be set up and managed with public network connectivity and optional private network connectivity with the OVHcloud Control Panel portal.
- **Virtual Machines (VMs)** may be created and managed individually using the OVHcloud Control Panel portal and customer vSphere instances, including storage.
- **Public and Private Networks** will be set up and managed with options such as edge gateway, internal networks, and NAT via OVHcloud Control Panel and customer vSphere instances. Network IPs, Dashboards, Load Balancers, vRack Private Network, and OVHcloud Connect are provided in support of the dedicated, private and public cloud servers.

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.

Principal Service Commitments and System Requirements

OVHcloud communicates commitments related to the security, availability, and confidentiality of the OVHcloud Services system via terms of service, data processing agreement, and service level agreements found on the us.ovhcloud.com public facing website. Commitments included within these agreements include the following:

- Maintain technical and organizational measures (including administrative, physical, and technical safeguards), internal controls, and data security routines to protect service data the OVHcloud Services system processes on the clients' behalf.
- Implement change management processes and procedures to maintain health and availability of systems, and to release hot fixes and security service packs.
- Provide incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to applicable infrastructure, service software, operating system templates, and tools provided by OVHcloud.
- Maintain availability of at least 99.0% on Dedicated Servers, 99.7% on Managed Bare Metal, 99.0% on Public Cloud instances, 99.50% on Managed Kubernetes Service, 99.95% on Hosted Private Cloud services, and 99.9% on Virtual Private Servers. (See https://us.ovhcloud.com/legal/service-level-agreements).
- Maintain cryptographic controls for the protection of confidential information.
- Confidential customer data is classified and handled in accordance with the Data Classification Policy and the Records Retention Policy.
- Customer data is purged from the OVHcloud Services system after 7 days from the customers' termination or non-renewal of contract date, unless customer requests 15 days to retrieve their data prior to contract termination.
- Production systems supporting the OVHcloud Services system comply with applicable NIST SP 800-53 guidelines.

OVHcloud communicates that customers retain ownership and control of their data within the OVHcloud Services systems; further, measures necessary to ensure the backup of the Customer's data remains the exclusive responsibility of the customer.

OVHcloud has also established system requirements that support the achievement of the principal service commitments and relevant laws and regulations. These requirements are communicated internally via the information security policies and procedures and externally via the public facing website and customer contracts. These requirements include the following:

- Logical and physical access controls over customer data.
- Automated ticketing system for tracking incidents and customer requests to resolution.
- Encryption of the virtual private network (VPN) and OVHcloud Control Panel and Application Programming Interface (API) Console.
- Backup media is encrypted at rest and access to encryption keys are restricted to authorized personnel.
- Routine vulnerability scans to identify and address risks / vulnerabilities for the systems used in delivering OVHcloud Services.
- Implement change management processes and procedures to maintain the stability, health, and availability of systems, and to release hot fixes and security service packs.
- Formal scripts and hardening configurations are deployed to the production systems.
- Monitor the availability, capacity, and performance of OVHcloud Services infrastructure, network infrastructures, top-layer management, user management interfaces, computing, storage, and network hardware.
- Automated processes are in place to purge customer data from OVHcloud systems when no longer in use.
- Undergo annual examinations by a third-party auditors to attest compliance with applicable NIST SP 800-53 guidelines.

In accordance with OVHcloud's 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 OVHcloud Services system is supported by infrastructure and software located in OVHcloud's US Data Centers and a third-party Data Center owned by OVH Group. The OVHcloud Data Centers are in Vint Hill, Virginia, and Hillsboro, Oregon; the third-party OVH Group Data Center hosting facility is in Beauharnois, Canada.

The production environment is administered remotely with access to the production environment being restricted to personnel via encrypted VPN connections configured to enforce two-factor authentication. Communication sessions are encrypted via advanced encryption standard (AES) 256. To protect data in transit, web servers transmit data utilizing hypertext transfer protocol secure (HTTPS) transport layer security (TLS) encryption.

The in-scope infrastructure consists of multiple systems as shown in the table below:

Primary Infrastructure			
Production System	**Business Function Description**	**Platform**	**Physical Location**
Bastions	Privileged identity and access authentication to in-scope infrastructure components.	Linux	Vint Hill and Beauharnois

Primary Infrastructure			
Production System	**Business Function Description**	**Platform**	**Physical Location**
Application, Web, and Database Servers	Production operating systems supporting OVHcloud Services and related systems.	Linux	Vint Hill, Hillsboro, and Beauharnois
vCenter	Server virtualization and management software that allows multiple virtual instances to share resources of a single hardware host.		Vint Hill and Beauharnois
Firewall Systems	Firewall systems in place to filter unauthorized inbound network traffic from the Internet.	Linux, Netfilter, and NSX Edge	Vint Hill, Hillsboro, and Beauharnois
OVHcloud Control Panel / API Console	Customer interface and orchestration tool that provides customers the ability to monitor and manage their services.	Linux	Vint Hill and Beauharnois
Data Center Badge System, Video Surveillance System, and Security Center	Internal system to manage and monitor physical access to Data Centers.		Vint Hill, Hillsboro, and Beauharnois

People

Personnel involved in the operation and use of the systems are:

- Executive Management (Senior Leadership) – responsible for overseeing company-wide activities; establishing and accomplishing goals; overseeing objectives, risk management and identification; and overseeing compliance of security issues and incidents throughout the service delivery infrastructure.
- Human Resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations, training, and professional development).
- Risk and Compliance personnel – responsible for managing security, availability, and confidentiality risks; performing or coordinating internal audits and communication of the results to Senior Leadership.
- Security Operations personnel – responsible for risk management and identification, monitoring, and compliance of security issues, file integrity monitoring, and security incidents throughout the service delivery infrastructure.
- Core Services personnel – are staffed 24x7x365 and responsible for monitoring and responding to alerts generated from the security monitoring applications, centralized logging system, and backup systems.
- Data Center Operations personnel – responsible for the installation of hardware, implementation of configuration changes, and troubleshooting incidents. Data Center Operations personnel are staffed 24x7x365 and are responsible for monitoring physical infrastructure components, environmental controls, and performing on-going maintenance.
- Product Business Units personnel – responsible for the software patch management, troubleshooting incidents, and on-going maintenance. The information technology (IT) operations teams maintain administrator access to the production environment.
- Customer Support – responsible for providing assistance and solutions to customers regarding products or services, including answering inquiries, resolving issues, and collecting feedback to improve the customer experience.

Procedures

Access, Authentication, and Authorization

Information Security Policies and procedures have been implemented to guide personnel in the protection of information assets, and supports the OVHcloud security program, which includes implementing and monitoring logical access, and security controls, including the following:

- Information Security Governance and Information Security Objectives Policies
- Data Classification Policy and Data Handling & Protection Standards
- Acceptable Use Policy
- Access Control and Authentication Policy

These policies and standards are reviewed and approved by management at least annually.

OVHcloud has bastions that function as the central point of control pertaining to identity and access management. Bastions are utilized to restrict access to production infrastructure and prevent users from directly authenticating into infrastructure components. Production infrastructure access is restricted to whitelisted Internet protocol (IP) addresses belonging to the bastions; as such, users must first authenticate to the bastion prior to connecting to production infrastructure.

Bastion users are authenticated via the use of cryptographic keys (private/public) and communication sessions are encrypted using the secure shell (SSH) protocol. Gatekeepers are responsible for assigning and maintaining access privileges within the bastion via use of a key distribution system (KDS). Users authenticate to the bastion host with their private SSH ingress key to establish an SSH connection. The bastion authenticates the user based on the public/private SSH key-pair and performs a permissions check for egress connection. To perform the permissions check, predefined security groups are defined to assign role-based access privileges within the bastion and restrict access to production infrastructure.

The bastion is utilized to assign user account privileges (i.e., SSH keys), based on security group membership, to log in with root access on various servers within the production environment. Root access within the bastion is restricted to authorized personnel. The bastion provides a mechanism to manage SSH keys to remote systems and allows users to access systems which provide traceability by recording the session. SSH sessions are programmed to terminate a session after a predefined period of inactivity.

A VPN connection requiring multifactor authentication is required to authenticate to the bastion. Additionally, vCenter and OVHcloud Control Panel are configured to enforce unique user accounts, multifactor authentication, and minimum password requirements. Administrators' access privileges to vCenter and OVHcloud Control Panel are restricted to authorized personnel from trusted source IP addresses.

Bastions and production servers are configured to log access and security related events, as well as send the logs to a centralized logging and monitoring security information and event management (SIEM) system. The centralized logging and monitoring system are configured to alert Security Operations personnel when predefined security events are detected, including privileged operations and account management activities. In addition, vCenter and OVHcloud Control Panel are configured to log user logon events; these events are reviewed by Security Operations personnel on an ad hoc basis.

User Access Administration

When a user requires access to information systems, Human Resources and the user's Manager initiates and authorizes a formal access request by submitting a user request ticket. If the request comes from a Manager level for the employee or above, the request is considered to have been authorized. Upon submission and authorization of the form, the request is routed to the system administrator team for approval and provision of the user access.

The process described above is applicable for new hires requesting access for the first time or for changes in access levels for existing employees in the event of a transfer or changes in job responsibilities.

User Access Removal

Human Resources sends notification of a user's termination to IT Support, and other 3rd Party administrator personnel for processing; upon receipt of the request, IT Support and 3rd Party administrator personnel disable the user's system accounts and disable SSH keys.

Periodic Reviews of Access

Compliance personnel perform a quarterly review of user access, including privileged user accounts, to ensure that access is maintained according to job responsibilities and management directives. The access review is documented and maintained as an auditable record. Discrepancies identified during the user access review are communicated to IT Support and Core Services personnel to be addressed accordingly.

Change Management

Changes to in-scope systems and infrastructure follow a standardized change management methodology. This methodology is documented in the Change Management Policies and procedures that are communicated to employees via the company intranet. Changes are categorized according to internal and external priorities. Changes are required to be authorized by internal and/or external personnel.

Changes are tracked in an internal ticketing system which contains information that includes but is not limited to the following:

- Type of Change
- Change Requestor
- Change Details
- Evidence of Testing, if applicable
- Change Advisory Board (CAB) Approval
- Implementation Plan, if applicable

Each change is required to undergo an impact analysis and have documented rollback plans; these are documented in the request for change (RFC) tickets. Prior to migration into the production environment, Operations personnel test the changes in a pre-production environment that is logically segregated from the production environment. Following successful testing, the change is reviewed by the CAB and is either approved or rejected for implementation and coordination of customer notifications, if required. Members of the CAB meet on a weekly basis to review and approve the change requests submitted for the week regardless of when the change is scheduled.

An implementation plan is documented within the RFC ticket and includes details of the change, tasks including related personnel and corresponding date/time of action, associated ticket numbers, expected results, and requested implementation date and time. Following approval, the CAB identifies Engineers responsible for the implementation of the change.

A configuration management tool and deployment servers are utilized to manage and maintain the in-scope systems and detect unauthorized changes. To implement changes to the production environment, changes must be staged within the configuration management tool for deployment. The ability to stage changes within the configuration management tool is restricted to authorized personnel.

If the change is deemed to impact customer services, Product business units will notify customers via the web portal the system will be unavailable during the specified maintenance window. The assigned Engineers perform the requested modifications as well as post-implementation testing.

Changes are required to be approved prior to implementation; required approvals are obtained by personnel commensurate with the impacted environment and known risk of interruption to services, as defined in the change management methodology. An abbreviated approval process is applied for changes classified as “Urgent”.

A file integrity monitoring tool is also in place and utilized to monitor for changes to critical in-scope systems and alert Security Operations personnel via e-mail, text messages, and pager alerts when predefined events occur. Security Operations personnel review the changes and perform an investigation in the event unexpected or unscheduled changes are identified.

Physical Security

Access to and within each Data Center facility is restricted via a badge access control system. The badge access control system is configured to enforce physical access privileges based on predefined security zones and access levels. Access to the production areas to the in-scope Data Centers is restricted using biometric authentication, as well as a mantrap with tailgating sensors.

The badge access system logs activity which is traceable to specific cardholders for ad hoc review by Data Center and Security Operations personnel for unauthorized access attempts and security violations. The ability to create, modify, or remove badge access users and privileges to the OVHcloud corporate facilities and Data Centers is restricted to user accounts accessible by authorized administrators. Physical access permissions are revoked by authorized personnel as a component of the termination process. Additionally, a video surveillance system is in place to record activity throughout the OVHcloud corporate facilities and Data Centers, and recordings are available for a minimum of 90 days for investigations.

Upon entering the Data Center facilities, visitors are required to present photo identification, register, and sign a visitor log, and must be escorted by an authorized employee and wear a visitor badge while on-site. The Data Center Physical Security Policy states that visitors must have a "business need" to access; accordingly, Data Center facilities do not permit unannounced visitors. Data Center Operations personnel monitor visitors' access to the Data Center facilities 24 hours per day, seven days a week. Visitor access records are reviewed on an annual basis and anomalies in visitor access records are reported to Data Center management.

Environmental Security

The OVHcloud Services system is supported by Data Centers in Vint Hill, Virginia, and Hillsboro, Oregon. Standard operating procedures are in place to govern environmental security practices at each of these facilities.

Fire, heat, and smoke detectors, audible and visual alarms, water sprinklers, and hand-held fire extinguishers are installed within the Data Centers to protect the facilities from the threat of fire. Redundant water cooling and air circulation systems are located within the Data Centers to regulate temperature and humidity levels. To protect servers from water damage and to help facilitate cooling, servers are located in raised racks and water detection systems are located under the water cooling and air circulation systems to detect leakage.

A building management system (BMS) is also utilized to monitor environmental conditions within the Data Centers and alert Data Center Operations personnel in real-time when predefined thresholds are exceeded for monitored devices. Data Center Operations personnel are staffed on a 24x7x365 basis to respond to alarms.

To provide temporary electricity in the event of a power outage, production equipment is connected to uninterruptible power supply (UPS) systems. The Data Centers are also connected to dedicated power generators that provide electricity during long-term power outages. The UPS systems have the capacity to support the Data Center load until the generators come on-line.

Environmental control systems and devices that support the OVHcloud Services system undergo preventive maintenance / inspections according to a predefined schedule. Third-party specialists are contracted to perform the US Data Centers' preventative maintenance / inspections of the following systems on an annual basis: fire detection and suppression systems, UPS systems, generators, and water cooling and air circulation systems.

Data Backup and Disaster Recovery

OVHcloud has implemented policies and procedures to guide personnel in performing data backups and data restoration. Procedures document each step of the scheduling, monitoring, quality assurance (QA), and restoration processes, as well as the associated roles and responsibilities.

OVHcloud utilizes an automated backup system to perform scheduled system backups of stateful OVHcloud servers. OVHcloud does not backup stateless servers as automation tools are configured to spin up a new virtual machine (VM) instance with the same configuration if an instance fails. System Engineers utilize the backup system to perform encrypted incremental backups of in-scope OVHcloud servers daily; and encrypted full backups are performed at least once every two weeks. Backup media is encrypted at rest and access to encryption keys are restricted to authorized personnel.

Administrative access privileges to the automated backup system and backup data, including encryption keys, are restricted to authorized personnel. The backup system records the results of each backup job as well as the associated date, duration, and size of the data backup. The automated backup system is also configured to alert Product Unit personnel via e-mail regarding the success or failure of backup jobs. In addition, production databases are replicated in real-time to databases within the Data Center to permit the resumption of IT operations in the event of a primary database failure. The backup system is also configured to backup databases daily to another Data Center more than 1,000 miles away which uses a different utility provider.

OVHcloud has documented a Disaster Recovery Plan to help guide personnel in responding and recovering from events that have the propensity to disrupt the organization's operations. The Disaster Recovery Plan is designed to achieve the following:

- protect employees, contractors, and those visiting the OVHcloud facilities;
- provide guidance for an immediate, accurate, and measured response to disruptive events;
- sustain OVHcloud's ability to meet customer commitments during disruptive events; and
- recover from disruptive events in accordance with customer commitments.

OVHcloud has formed a disaster recovery team that is comprised of Senior Leadership and Product Business management. The team meets annually to evaluate and test the plan to help ensure its continued suitability. Additionally, Systems Engineering personnel perform a restoration of backup files at least annually to ensure system recovery.

System Monitoring and Incident Response

A firewall system is installed and utilized to protect the production environment and data. The firewall system resides on the network perimeter and analyzes data and packets routed to the OVHcloud network supporting the OVHcloud Services system. External Internet traffic is required to pass through the firewall system to communicate with the production infrastructure. Security Operations personnel are responsible for reviewing firewall rule documentation, perimeter testing, and monitoring the firewall system to reduce the likelihood of unauthorized, malicious, or unintentional interception of data in transit. Implemented configurations include the access policy being set to "deny" by default. Therefore, any type of connection that is not explicitly authorized by the firewall system will be denied. The firewall systems require administrators to authenticate via a user account and password, as well as two-factor authentication to access the firewall system rulesets. Also, failover services are enabled in the event of a primary firewall system failure.

The ability to modify the firewall system software, configurations, or rulesets is restricted to user accounts accessible by authorized personnel. Cores Services and Product Business unit personnel utilize a ticketing system to track and manage changes or updates to the ruleset. If an additional firewall rule needs to be added, Core Services and Product Business personnel document the business justification for the change in the associated ticket.

Security Operations personnel utilize an intrusion detection system (IDS) to monitor the in-scope servers for suspected or actual security breaches. The IDS is configured to log predefined events, including events originating from the same IP address, events with the same source and destination IP address, events with the same source to multiple destination IP addresses, and repetitive attempts within a certain amount of time.

A centralized logging system is also in place that aggregates event logs from the in-scope systems and alerts Security Operations and Core Services personnel via e-mail when predefined events are detected.

In the event a suspected or actual security incident is discovered, Security Operations personnel work to contain and resolve the incident, and works with other subject matter experts (SMEs) to determine the cause of the breach. Once the incident is resolved, Security Operations personnel log the resolution and remediation activities in a ticket, as well as conducts a post-mortem assessment. Any changes to the IDS configurations and rulesets are also noted in the ticket.

Security Operations personnel utilize an automated ticketing system to document security violations, responses, and resolutions. Upon receipt of the alerts, Security Operations personnel review the alerts to determine if any additional action should be taken.

A patch management methodology is in place to guide personnel in the initiation, testing, and deployment of patches for in-scope infrastructure. Operating system security patches are applied on an automated weekly basis. Patch and/or upgrade notifications for other software are received from the software vendors or internal parties and evaluated for prioritization based on the type of patch (e.g., security related patches are applied more frequently).

Antivirus software is utilized to protect registered devices (i.e. workstations) and configured to monitor for updates to virus definitions at least daily. The antivirus software is also configured to scan registered workstations on-access. The antivirus software is also configured to scan registered Microsoft servers at least weekly.

Enterprise monitoring applications are in place to monitor the performance and availability of production systems including current processing capacity and use of system components. The enterprise monitoring applications display monitored device metrics in the control room of each in-scope Data Center; the control room is staffed with Data Center Operations personnel on a 24x7x365 basis to monitor the device metrics.

Core Services and Product Business unit personnel monitor the system for incidents 24 hours per day and tracks incidents via the ticketing system for monitoring and resolution. The enterprise monitoring application is configured to alert Core Services and Product Business unit personnel via a pager system when predefined thresholds are exceeded.

A BMS is also utilized to monitor environmental conditions within the Data Centers and alert Data Center Operations personnel via on-screen alerts when predefined thresholds are exceeded for monitored devices.

- fire alarm status and suppression systems; and
- temperature and humidity levels.

Data

OVHcloud has a documented Data Classification Policy and Data Handling and Protection Standards in place that defines data within the following categories:

- Public – applies to information that is available to the public and is intended for disclosure to the general public. This information has no access restriction and may be freely disseminated without potential harm.
- Confidential/Internal – applies to information that has significant impact on business, but its disclosure would result in moderate level of risk and is unlikely to result in financial loss or serious damage to OVHcloud's credibility. This information is available to company employees based on their job classification or responsibility ("role-based" access).
- Private/Protected/Highly Restricted – applies to information available to a privileged team of OVHcloud employees on a "must know" basis. Its disclosure could result in an extreme level of risk to the Company, its affiliates, its employees, and its customers.
- Restricted – applies to the most sensitive business information intended strictly for use within OVHcloud, with access only available to a privileged team of OVHcloud employees on a "need to know" basis; logging of access is enabled where feasible. Unauthorized disclosure could lead to catastrophic damage to the organization, employees, and business partners.

OVHcloud employees sign non-disclosure agreements during the on-boarding process. Internal access to systems that house confidential customer information is restricted to authorized personnel who require such access to perform their job functions. OVHcloud employees are required to acknowledge, upon hire and annually thereafter, that they have read the OVHcloud Code of Business Conduct & Ethics and the US Employee Handbook, which contain information regarding information security practices and customer confidentiality.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer Data processed by the system	OVHcloud Control Panel / API Console	Restricted
Customer Profile and Billing Information		
Badge Access Logs	Logged Activity for the Badge Access System	Private
Security Camera Surveillance Images	Surveillance Activity pertaining to Physical Access to the Data Center facilities	

Significant Changes During the Period

During June 2025, OVHcloud began migrating their data and systems hosted by OVH Group's Data Center located in Beauharnois, Canada, to the OVHcloud Data Center located in Vint Hill, Virginia. The migration was completed during December 2025, at which point the data center hosting services provided by OVH Group were no longer utilized by OVHcloud.

The aforementioned migration of data and systems to the Vint Hill, Virginia, data center did not affect the design or implementation of control activities relating to the OVHcloud Services system. Additionally, the change had no impact on the application development services provided by OVH Group, which continued to be utilized by OVHcloud throughout the period.

Subservice Organizations

The data center hosting and application development services provided by OVH Group 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 OVH Group, alone or in combination with controls at OVHcloud, and the types of controls expected to be implemented at OVH Group to achieve OVHcloud's principal service commitments and system requirements based on the applicable trust services criteria.

Control Activities Expected to be Implemented by the Subservice Organization	Applicable Trust Services Criteria
OVH Group is expected to implement controls that ensure physical access is restricted to the Beauharnois, Canada, Data Center facility.	CC6.4 – CC6.5
OVH Group is expected to implement controls that ensure the development and implementation of patches and required maintenance to OVHcloud Control Panel / API Console.	CC8.1
OVH Group is expected to implement controls that protect data center hosting services from environmental threats and for monitoring environmental conditions within the Beauharnois, Canada, Data Center	A1.2

Complementary User Entity Controls

OVHcloud'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.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the OVHcloud Services system.