APPENDIX

Technical and organizational measures adopted by the Processor

1. Security and Management System

An IT systems security policy (ISSP) is put in place that sets out all the provisions we take in this regard. Our ISSP is updated every year, at the minimum, or every time there is a major change that has ramifications for its content. The security of our solutions is assured by formal information security management systems.

Various roles coordinate our actions with regard to the security of the perimeter: the IT system security manager (ISSM); the security manager, responsible for processes and projects associated with the security of the perimeter; the data protection officer (DPO), who is in charge of preserving personal data; the risk manager, who coordinates the management of security risks and the associated action plans; and the security measures manager, who implements and applies the provisions pertaining to the risks identified.

2. Risk Management

A formal methodology for risk management is put in place. This is reviewed annually at the minimum, or in the event of a major change. It also concerns personal information and sensitive data (health, payments, etc.). This methodology formalizes the analyses carried out. It identifies assets, critical industry processes, threats and vulnerabilities. It is based on the ISO 27005 standard. A plan for handling any risks identified is devised following each analysis. This plan is then implemented within a maximum of 12 months. It documents the analysis in detail and sets out the order of priority for the actions to be taken. Each corrective measure is added to the action plans and is covered by a formal, tracked follow-up, together with a regular review to reexamine its effectiveness.

3. Change Management

A formal change management procedure is put in place: roles and responsibilities are clearly defined; criteria for classification are set out in order to identify the steps to follow as part of implementing the change; priorities are managed; the risks associated with the changes are analysed (if a risk is identified, the security manager and risk manager work together to validate the change); intrusion tests may be carried out (where applicable); the change is planned and scheduled with the customers (where applicable); the change is rolled out gradually (1/10/100/1000) and, if there is a risk, a rollback procedure must be planned for; a retrospective review of the various assets concerned by the change is carried out; all steps are documented in the change management tool.

4. System and application development policy

Processes for OVH developers are set up and documented. These processes contain the principles of secure development, “privacy by design” measures, and a code review policy (vulnerability detection, error processing, managing access and entry and protecting storage and communications). Code reviews are also carried out on a regular basis; new features are validated prior to launch, tested in a validation environment (where applicable) and rolled out gradually (1/10/100/1000); a distinction is drawn in terms of roles and responsibilities between developers and the persons responsible for launching production.

5. Monitoring Services and Infrastructures

A monitoring infrastructure is implemented for all OVH services. This has several objectives: to detect production and security incidents; to monitor critical features, with any alerts being escalated to the monitoring system; to inform the persons responsible and trigger the appropriate procedures; to ensure continuity of service in the performance of automated tasks; to ensure the integrity of the resources monitored.

6. Incident Management

An incident management process is set up. This process is used to prevent, detect and solve issues in the service and its management infrastructures. The process includes: a guide for classifying security events; handling security events; simulation exercises for the crisis unit; customer communication as part of a crisis unit. These procedures are covered by a continuous improvement process for the monitoring, assessment and overall management of incidents and their corrective actions.

7. Vulnerability Management

Technological monitoring for new vulnerabilities is carried out by the security manager and their teams. These vulnerabilities are identified via: public information sites; alerts from the manufacturers and publishers of the solutions deployed; incidents and observations escalated by our operations teams, third parties or customers; internal and external vulnerability scans performed on a regular basis; technical audits and code and configuration reviews. If a vulnerability is detected, it is analysed by dedicated teams in order to determine its impact on the systems and the potential operating scenario. Mitigation measures are implemented, where necessary, and a corrective plan is then defined. Each measure taken is added to the action plans and is covered by a formal, tracked follow-up, together with a regular review to reexamine its effectiveness.

8. Natural and environmental risks

Measures are implemented to prevent natural and environmental risks: lightning rods are installed to reduce the concomitant electromagnetic radiation; OVH offices are set up in zones not subject to flooding or the risk of earthquakes; uninterruptible power supplies (UPS) of a sufficient capacity and emergency transformers with automatic load-switching; automatic switching to electricity generators with a minimum autonomy of 24 hours; a water-cooling

system is used for servers (98% of our hosting rooms have no air conditioning); heating, ventilation and air conditioning (HVAC) units are used to maintain temperature and humidity at constant levels; a fire detection system is in operation (fire drills are run every six months in datacentres).

9. General security measures for physical sites

Physical access to OVH sites is based on a restrictive perimeter security system, which applies from the entrance area onwards. Each site is divided up as follows: private traffic areas; offices accessible to all employees and to registered visitors; confidential offices, for authorized personnel only; areas containing datacentre equipment; confidential areas in datacentres; areas in datacentres hosting critical services.

Security measures are taken to regulate access to OVH's physical sites: an access permissions policy; walls (or equivalent dispositions) between each area; cameras located at the entrances and exits to installations, as well as in the server rooms; secure access, controlled by badge readers; laser barriers in the car parks; a motion detection system; burglary prevention systems at the entrances and exits to datacentres; intrusion detection mechanisms (security guards 24 hours a day and video surveillance); a permanent surveillance centre monitoring when the entrance and exit doors are opened.

10. Access to OVH Sites

Physical access control operates using a system of badges. Each badge is linked to an OVH account, which, in turn, is linked to an individual. This system makes it possible to identify all persons within the installation and to authenticate the control mechanisms; every individual entering an OVH site must have their own individual badge associated with their identity; the identity of every person must be verified before any badge is issued; within the installations, badges must be worn in a visible location; badges must not show the name of their owner or the name of the company; badges must makes it possible to identify the categories of persons present (employees, third parties, persons with temporary access, visitors); badges are deactivated as soon as their holders are no longer authorised to access the installations; OVH employees' badges are active for the duration of their employment contracts; for the other categories of person, badges are deactivated automatically after a defined period; any badge that is not used for a period of three weeks is automatically deactivated.

11. Area Access Management

Door access via badge This is the standard form of access control at OVH: doors are connected to a centralised access rights management system; people have to badge in using a dedicated badge reader in order to unlock the doors; access rights are verified when the badge is read, to ensure that the person in question has the requisite entry rights; if the centralised access rights management system goes down, the rights configured at the time of the incident will remain valid for its entire duration; door locks are protected against power cuts and will remain locked if there is no power.

Door access via key Some areas or items of equipment are locked using key locks; the keys are stored in a centralised, access-restricted location on each site, with a reference document; each key is identified via a label; an inventory of the keys is kept; any use of the keys is traceable, via a delivery mechanism or a paper journal; the reference document for the keys is checked against the inventory every day.

Access to datacentres via single-person airlocks Our datacentres are accessed exclusively via single-person airlocks: each airlock has two doors and a delimited area between the checks, to ensure that only one person gets through at a time; each door will not open unless the other door is closed (*mantrap*); *the airlocks use the same system of badges as the other doors, and the same rules apply to them; detection mechanisms verify that there is only one person in the airlock (*anti-piggybacking*); the system is designed to make sure badges cannot be used more than once in the same direction (*anti-passback); a camera placed next to the airlock means that people entering can be monitored.

Access to the goods airlocks Access to the datacentres for goods is exclusively via dedicated walkways: the delivery vestibule is configured in the same way as a single-person airlock, larger in area and with no verification of volume or weight, and with badge readers on the outside only; only the item being delivered passes via the vestibule - accompanying personnel must enter via the single-person airlocks; there is a camera in the vestibule, with no blind spot.

12. Third Parties Physical Access

The movements of visitors and ad hoc service providers is strictly supervised. These persons are logged as soon as they arrive on site and are issued with a visitor or a service provider badge: all visits must be announced ahead of time; third parties are the responsibility of an employee and must be accompanied at all times; all identities are verified prior to granting access to the site; each third party is issued with a staff badge, allocated to them for the day, which they must return before leaving the site; all badges must be worn in a visible manner; badges are automatically deactivated at the end of the visit.

13. Network security

OVH manages its own network of high-performance fibre optic lines, connected to numerous operators and forwarding agents. OVH backbone distributes connectivity to each datacentre's local networks and connects the datacentres to each other. All this equipment is secured using the following measures: an inventory is kept within a configuration manager database; a tightening process is in place, featuring guides that describe which parameters need to be modified in order to ensure a secure configuration; access to the administrator features for equipment is reserved to staff listed on control lists; all equipment is administered via a bastion host, applying the principle of least privilege; all configurations for network equipment are backed up; the logs are collected, centralised and monitored on a permanent basis by the network operations team; configurations are deployed automatically, based on validated templates.

14. Personnel training and awareness

OVH personnel follow security awareness training and are trained in compliance rules for personal data processing: training sessions on these topics are organised annually for the teams concerned; training sessions on carrying out audits are organised annually for the teams concerned; training sessions on the technical services are organised annually for the teams concerned; awareness training in IT system (IS) security is organised for new employees when they join the company; messages about security are regularly sent to all personnel; test campaigns are organised to ensure that employees know how to act in the event of a threat.

15. Managing Logical Access to OVH IT System

A strict policy of logical access rights management for employees is applied: authorisations are issued and monitored by managers, following the principle of least privilege and the principle of gradually gaining trust; to the extent possible, all authorisations should be based on roles rather than unit rights; the access rights and authorisations granted to a user or to a system are managed based on a procedure of logging, modification and delogging that involves the managers, internal IT and human resources; all employees use nominative user accounts; connection sessions systematically have an expiry period suited to each application; users' identities are verified prior to any change in authentication methods; if a user forgets their password, only their manager and the security manager are authorised to reset it; user accounts are automatically deactivated if the password is not renewed after 90 days; the use of default, generic and anonymous accounts is prohibited; a strict password policy is applied; users use automatic password generators rather than choosing their own passwords; the minimum length for passwords is 10 alphanumeric characters; passwords must be renewed every three months; storing passwords in unencrypted files, on paper or in web browsers is prohibited; the use of local password management software, which has been approved by the security teams, is mandatory; any remote access to the OVH IT system (IS) must be via VPN, using a password known solely to the user and a shared secret key configured on the workstation.

16. Managing administrative access to production platforms

A policy for managing administrator access rights for platforms is applied: all administrator access to live systems is realised via a bastion host; administrators connect to the bastion hosts via SSH, using individual and nominative pairs of public and private keys; connection to the target system is realised either via a shared service account or via a nominative account and bastion hosts; using default accounts on systems and equipment is prohibited; dual-factor authentication is mandatory for remote administrator access and for any employees accessing sensitive areas of the system, with such access being fully traced; administrators have an account exclusively devoted to administration tasks, in addition to their standard user account; authorisations are granted and monitored by managers, in accordance with the principle of least privilege and the principle of gaining trust; SSH keys are protected by a password that meets the requirements of the password policy; access rights are reviewed on a regular basis, in collaboration with the departments concerned.

17. Managing Access to Control Panel

Customers can manage their OVH services from their Control Panel or the API. Default access is via a nominative account (NIC handle) and a password; the password is chosen by the customer and must meet the complexity criteria imposed by the interface; only the hashes of the passwords are stored on OVH's servers; OVH offers the option of activating dual-factor authentication via the Control Panel, using a system of one-time passwords (OTP) sent by SMS, a mobile application, or a U2F-compatible key; customers may restrict access to their Control Panel to certain predefined IP addresses; the API's access tokens are usable for as long as they remain valid, and no specific subsequent verifications need to be applied; all customer activity in the Control Panel or the API is logged; customers can choose to handle the technical and administrative tasks associated with the management of their services separately.

18. Security for workstations and mobile equipment

Protection of standard workstations Measures to protect the standard workstations of OVH personnel are in place: updates are managed automatically; antivirus software is installed and updated, and regular scans are carried out; only those applications contained in an approved catalogue may be installed; hard drives are systematically encrypted; employees do not have administrator rights on their workstations; potentially compromised workstations are handled according to a specific procedure; equipment is standardised; there is a procedure for deleting sessions and resetting workstations when employees leave the company.

Protecting mobile terminals Measures to ensure the security of mobile terminals, whether belonging to personnel or supplied by OVH, are in place: terminals must be registered in a centralised management system before they are granted access to internal resources (WiFi, email, calendars, people directory, etc.); the security policy used on the terminal is verified (unlock code, lock time, storage encryption); procedures are in place for wiping the terminal remotely if it is lost or stolen.

19. Logging

A logging policy is in place for the servers and equipment used by OVH to deliver its services: logs are backed up and centrally conserved; logs are consulted and analysed by a limited number of authorised personnel, in accordance with the authorisation and access management policy; tasks are divided up between the teams responsible for operating the monitoring infrastructure and the teams responsible for operating the service. The list of activities that are logged includes the following: logs of storage servers hosting customer data; logs of the machines managing the customer's infrastructure; logs of the antivirus software installed on all equipped machines; integrity checks of logs and systems, where appropriate; tasks and events carried out by the customer on their infrastructure; logs of network equipment; logs of the infrastructure of the surveillance cameras; logs of administrator machines; logs of time servers; logs of badge readers; logs of bastion hosts.