DESCRIPTION SAAS HOPEX

SERVICES DESCRIBED HEREIN ARE ONLY APPLICABLE TO THE STANDARD VERSION OF HOPEX. IF THE CUSTOMER WISHES THEM TO BE APPLICABLE TO SPECIFIC DEVELOPMENTS AND CUSTOMIZATIONS, THE PREMIUM MAINTENANCE OPTION MUST BE SUBSCRIBED TO.

CUSTOMER IS ADVISED THAT REFUSAL TO MIGRATE TO A SUPPORTED VERSION, IN ADDITION TO NOT BENEFITING FROM MAINTENANCE SERVICES INCLUDING DELIVERY OF PATCHES, EXPOSES TO SECURITY ISSUES. MEGA SHALL NOT BE LIABLE FOR ANY CONSEQUENCES THAT COULD HAVE BEEN AVOIDED HAD CUSTOMER MIGRATED TO A SUPPORTED VERSION OR ACCEPTED THE INSTALLATION OF A CORRECTIVE PACK OR HOTFIX.

1. DEFINITIONS

TERM	DEFINITION
Specific development / Customization	Any specific development or parameterization of HOPEX product which modifies functionalities according to Customer’s specific functional requirements. Modifications can relate to the data structure, screens, workflows, data access rules, interfaces requiring development, specific exports such as an intranet website or complex reporting requiring programming. User management and configurations made by end users (such as display preferences, queries, standard reporting features) are not addressed as customizations, but only basic configuration of the standard product.
Error	Behavior of Service which does not comply with Documentation. Any error should be reproducible, have clearly identifiable symptoms and generate functional consequences on the standard service.
Workaround	Alternative operating mode to overcome an Error.
Incident	Behavior which is not part of the standard operation of the services, and which interrupt the Service in production or decrease the quality of the Service.
Case	Instance used by MEGA technical support to follow an incident raised by Customer.
Service Unavailability Period or Outage	The time interval within the period of applicability of the Service Level Agreement during which the Service is unavailable to users.
Release or New Version	New version of the software, including new features.
Fix	Modification of Service, developed by MEGA to fix an Error. Corrections are usually bundled in a Corrective Patch or sometimes provided through a Hotfix.
Corrective Packs of CP or Minor Version	Means updates to make HOPEX more reliable. CP provides a consistent set of fixes, as well as security and performance improvements applicable to a Long-Term Support release.
Hotfix	Fix set and provided by MEGA outside the context of a Release or a CP. Hotfixes usually respond to Critical Errors and can only be installed on the last CP of a Release.

2. ACCESS TO THE SERVICE

Access to the service is limited to predefined IP addresses provided by Customer. IP addresses must be public (routable), static and listed IPs.
Roaming users will first connect to a Customer's relay site, which will provide them with an IP address that MEGA allows access to, and then connect to the Service.
Customer further immediately reports any incident to MEGA concerning access to the Service. Customer has not to interfere with or disrupt the service, including MEGA's or MEGA’s hosting provider servers, and complies with recommendations, procedures and rules communicated by MEGA from time to time for the appropriate use of the Service.

3. USER CREDENTIALS

MEGA will provide the user credentials to allow Customer administrator, the one responsible to set up credentials for other users.

Customer must take all necessary measures to ensure the confidentiality of the user's credentials. MEGA is not be liable for any damages resulting from the use of the service by an unauthorized third party. In the event of loss or disclosure by a user of his/her login information to an unauthorized third party, Customer shall notify MEGA in writing without any delay. For security reasons, MEGA may at any time require Customer to change a password or delete a user ID without prior consent.

4. SERVICE AVAILABILITY

MEGA will use reasonable efforts to make services available as set forth therein, except:

- During maintenance periods. Scheduled maintenance is subject to reasonable notice, while unplanned maintenance will be subject to 1 business day notice (except in case of Security Incidents);
- As a result of any circumstances beyond MEGA's control, such as Internet disruption and any other event of Force Majeure;
- In the event of any security problem, such as abnormal, fraudulent or abusive use of the services, any intrusion, fraudulent access to the services by a third party, or illegal data extraction of all or part of the data, etc., Customer is liable to pay costs incurred by services.

MEGA will use its best efforts to minimize the consequences and restore the Service after the above causes have ceased.

SERVICE AVAILABILITY	DEVELOPMENT	PRODUCTION
Maximum unscheduled outage duration	1 business day	3 business hours
Maximum monthly unscheduled outage	1 business day	4 business hours

All unavailability periods are computed in calculation of outage set forth above, except:

- Scheduled unavailability periods, such as periods authorized in advance by Customer as part of change management operations
- Unscheduled unavailability periods resulting from disclaimer set forth in this section.

The interruption is computed from the moment Customer contacts MEGA: declaration of a *No Access* from the Support section of our Community (https://community.mega.com).

In the event of non-compliance with availability commitments, Customer may request a service credit. A service credit represents the number of additional days of Service (in addition to the current subscription period) granted to Customer for outage. Any service credit has to be requested in writing. Such request must be made within the 3-month period following the date of the generating event. Service credit is Customer's sole and exclusive remedy in the event of service unavailability.

The period of availability of the Service is from 9am to 6pm, Monday to Friday, excluding banking holidays.

5. LIMITATION OF MEGA’S LIABILITY

MEGA’s liability shall be limited or excluded in the following cases:

- Customer’s failure to follow instructions for use of the service as set out in Documentation and user's guide;
- Performance degradation due to Customer network configuration and security devices;
- Incident due to a software product installed on Customer’s computing system.
- Unavailability of a Customer’s point of contact during an outage.
- Customer Refusal to promptly provide information (or authorization to access it) that might allow MEGA to fix an Incident or an Error.

6. INCIDENT SEVERITY & RESPONSE TIME

SEVERITY	SITUATION	RESPONSE TIME & EXPECTATION
No Access	Security issues Platform down/No access for all users	1 Business Hour
Critical	Significant degradation of one or more functionalities Critical business impact	Customer contacted within 4 working hours. Daily continuous effort during working hours. Quick escalation to the technical support and to product managers. Quick allocation of appropriate resources. Set up of a remediation plan. Depending on the complexity of the Error, a Workaround may be provided to minimize operational disruption.
Moderate	Degradation of functionality. Work may continue satisfactorily, but impaired. Moderate business impact Moderate business impact.	Customer contacted within 1 business day. Allocation of resources to maintain a constant effort during working hours. A remediation plan can be provided.
Minor	Minor degradation of one or more functionalities. No business impact.	Customer contacted within 2 business days. Best efforts during business hours.

A response time is calculated from the day after Customer notifies MEGA of Error via the Support Center accessible from Online Community.
MEGA's technical support may lower the severity level if Customer is unable to provide resources or responses necessary to allow MEGA to continue its efforts to resolve the Incident.
Standard support services do not include on-site assistance. In specific cases, and after approval by Customer of terms and conditions of MEGA's intervention, MEGA may intervene on Customer's site at its discretion. Customer provides MEGA with access to Customer's resources and sufficiently qualified personnel to give any information it may require. Customer makes available data required for support and ensure that it has all the intellectual property rights on the third party items made available to MEGA.

7. LIFE CYCLE POLICY

DEFINITION	DESCRIPTION
Release (Long-Term Support)	New version of Hopex maintained during the following periods: in Full Support for a 27-month period, then in Limited Support for 9-month period, and regularly enhanced by CP. Specific duration for each versions are available on MEGA community.
Full Support	Period during which Customer receives maintenance and support services including enhancement of existing features, addition of new features and products, and Patches.
Limited Support	Period following the Full Support period, during which Customer only Critical Incident may be fixed through Hotfixes only.

8. BACKUP AND DISASTER RECOVERY PLAN (DRP)

8.1. Backup.
As part of the (non-optional) hosting services, MEGA agrees to perform the number of data backups set out in this section.
In the event of a disaster affecting its hosting servers, MEGA agrees to restore the Services within the timeframe defined in this document.
By default, restoration is performed from the last backup. All other backups kept according to terms of this document are considered as archives and can be restored.

BACKUP	DAILY	WEEKLY	MONTHLY
Retention period for backups from a periodic backup	7 days	4 weeks	6 months
Time to restore	Last backup: 4 business hours Archive: 6 business hours		

8.2. Disaster Recovery Plan.
Customer benefits from a Disaster Recovery Plan in the event of Error affecting database or a problem affecting servers hosting the Platform, solutions and/or Customer's data.
MEGA is committed to:

- Perform backups of Customer's data according to a predefined frequency. This latter refers to the last backup, which is used by to perform its recovery plan (RPO),
- Restore Customer's data from the last backup within the timeframe defined below. This recovery time (RTO) required by MEGA to restore the services.

Customer may subscribe, at its sole discretion, to the "Advanced DRP" option to benefit from higher frequency backups and/or shorter recovery time.

	Recovery Time Objective (RTO)	Recovery Plan Objective (RPO)
Standard offering	1 week	25 hours
With Advanced DRP option	24 hours	25 hours

9. PENETRATION TESTING

MEGA will conduct annual third-party penetration testing of its SaaS Service. Such testing will be performed on the Full Support Releases (last CP), available on the market on the day of the penetration testing. Any other demand of the Client may be subject to additional fees. Upon request, MEGA will provide Client with an opinion letter and a summary report of the results of such penetration testing.

10. SERVICE REQUESTS

A Service Request is a formalized request for intervention on Customer's SaaS platform(s).
The only persons authorized to perform Request Services are those designated by Customer as "MEGA Contacts".

10.1. Services included in standard.

Service Category	Department name	Description of the Service	Frequency/Quantity max	Response Time
Version management	Application update	Deploy a HOPEX update on one of the SaaS platforms (DEV; PRE-PROD; PROD); HotFix, Patch, Release.	4 per year	HotFix, Corrective Patch 2 business days (PPROD first) Version Must be planned in advance
User Management	User login	Provide a log file (TXT format) stating all user connections including user licenses, usernames, profiles, and platform availability.	1 per month	1 business day
	Reassign a user/profile to a token license	With named licenses, reassign a user to a token-based license model. A user can be: main user, contributor or reader. This service does not apply to floating licenses.	10 reassignments (all users) per year	
Access Management	Change the domain name of the service	Change access URL to HOPEX Cloud from a domain name "aaa.hopexcloud.com" to "bbb.hopexcloud.com".	2 changes per year	2 business days
	Declare additional IP address ranges on the allowed access list	Add up to 5 additional IP address ranges to the list of IP addresses that are allowed to access the HOPEX Software Package.	3 requests per year	1 business day
Integration Management	Task scheduling	Schedule recurring tasks with upload or download (if applicable) to and from Customer's environment using a Secure File Transfer Protocol (SFTP). Scheduled tasks are mainly import/export and static web site generation. Design, make and validate items to be planned remains under the responsibility of Customer.	6 requests per year	2 business days (PPROD first)
	Deployment of Web Services	Deploy a Web Services in production. Design, make and validate a Web Service remains the responsibility of Customer.		3 business days (PROD first)
HOPEX Store	Deployment of a module	List of evolving modules: https://store.mega.com/modules	10 requests per year	2 business days (PPROD first)

Service requests are subject to this Service Level Agreement.
Any change in the frequency and/or maximum quantity of service requests is subject to additional charges.
In addition, MEGA may only be committed to service requests if:

- Service request is open from the MEGA Community website (no service request sent by email will be processed);
- MEGA Contact acknowledges that he/she has provided MEGA with all the information necessary to implement a service request. Time required to collect information will be deducted.

For requests not listed in the Service Request catalog:

- Estimated response time within 2 business days
- Study and treatment according to the request

10.2. Service levels of the "SaaS Platform Package".

Service Levels	Type of platform	Number of move to production
Starter	Pre-production and production	1 per year
Standard	Development, pre-production and production	4 per year
Advanced	Development, pre-production and production	12 per year

11. EXTENDED SERVICES OPTIONS

MEGA proposes a series of optional services in the SaaS subscription, including premium maintenance, adoption services and administration services, as described below. These services are called Extended Services and aim to provide customers with a premium support and post-implementation experience.

11.1. Premium Maintenance

Object	Description
Premium Support	
Proactive monthly follow-up	Monthly meetings to report on Case resolution with a single point of contact
Monitoring of health indicators	Monthly review of health indicators including number of Cases & SLAs.
Maintenance of customizations	
Correction of configurations/customizations including documentation	Support and correct the modifications that have solely been made by MEGA. This also includes the modifications required to upgrade the service.
Upgrade management	
Upgrade-Functional validation	Perform functional validation of configuration after upgrading to the latest HOPEX version.
Manage the impact of minor releases on users	Assess the impact of any user upgrade change on the user base. This will result in activities such as communication with users and the identification of users who require additional training.

11.2. Adoption Package

Object	Description
Maturity assessment and monitoring	
Maturity assessment workshops	Functional workshops each year aimed at improving adoption, usage of HOPEX and value demonstration, based on MEGA maturity assessment methodology, including one presale expert and one CSM
Follow-up of recommendations	Monitoring of HOPEX adoption through key indicators. and implementation of expert recommendations
e-Learning	
eLearning sessions	eLearning sessions to increase adoption within the team

11.3. Managed Services

Object	Description
Access management	
Management of the HOPEX authentication mode	Manage HOPEX authentication mode of HOPEX users.
Manage business roles	Assign business roles. A business role defines the function of a person or a person group in the enterprise. A business role is defined at a repository level.
Manage person groups	Set up, remove and configure group of persons into a group which shares the same connection. A Person Group is a list of persons belonging to the same group.
User access/group management	Set up, remove, configure users, user group, user profile, access and authorization levels.
Define data access rules	Set up, remove and configure user authorization structures.
Reset a user password	Set/reset user password (this only includes password reset for MEGA users).
Content Management - User Work	
Manage duplicate objects	Identify duplicate objects (working with content owners), validate duplication and perform actions to remove duplicates i.e. merge or deletion.
Manage isolated objects	Identify isolated objects to allow assignment of ownership, identification for deletion, report of objects not on diagrams (where expected to be described by diagrams), report on objects not included in associations.
Manage objects for deletion	Delete objects, where the modelling user has no privileges to delete objects created outside of their current transactions. Objects can be marked for deletion by users.
Manage merge of objects	Merge objects (i.e. duplicates) within a repository.
Manage data access	Set up and maintain object authorization levels that allow/disallow modification of objects by a specific user/user profile.
Manage object protection	Activate or deactivate protection of specific objects within a repository.
Content Management - Administration	
Compare and align repository/subset of content	Compare and promote objects/scope of objects from separate repositories. The target repository can be aligned with the base repository.
Logical backup of content group	Create a logical baseline for a specific content group (scope i.e. library, project etc.), enabling the creation of independent baselines of segments of the repository content.
Manage libraries	Set up and maintain libraries and ensure a clear content structure within the repository. Libraries may be used to logically separate repository content.
Create queries and reports	Write queries that are registered and available to all users in the environment to re-use. Configure reports based on Report Studio capabilities.
Workflows management	Manage workflows transition to support object approval, authorization and movement. Monitor workflow actions and reassignments.
Data import	Manage regular import of data using existing XLS templates.
Incident management	
Manage internal support	Manage first level of support on customer's functional use Cases, in a custom platform context.
Manage Case follow-up	Create, prioritize and follow-up Cases with MEGA Technical Support. Provide them all the necessary elements to diagnose the issue raised.
Coaching and support	
Guidance	Provide best practices and standard guidance on HOPEX usage
Model transcription	Manage manual transcription of existing models (MS Word, PPT, Visio, …) or of structured data (XLS format) to HOPEX Not applicable for mass loading.
Manage diagraming maintenance	Update existing diagrams based on a formalized change request. Manage impact on drawings from changes on core data concepts.
Guidance	Provide best practices and standard guidance on HOPEX usage
Integration and training of users	Integration and training of new users based on existing documentation and training materials.
EA Modeling	From interview of SME to validation of your EA asset on HOPEX diagrams
Users onboarding and training	Onboard and deliver training to new end-users based on existing customer training course and documentation.
Ongoing evolution	
Configuration	Evolution of existing configuration.

12. CONTACTS AND GOVERNANCE

Upon execution of the Agreement, Customer appoints a maximum of 3 designated contacts, trained on services, and to whom MEGA will provide support services. Designated contacts must be able to perform at least the following functions:

- Manage users and their assignment on different profiles of the MEGA solution(s) constituting the Service;
- In case of an Incident:
  - Declare a Case on MEGA portal by collecting and providing all necessary information related to circumstances in which the Incident occurred;
  - Report any security issue immediately by the most appropriate means;
- For greater operational efficiency, participate in management and arbitration meetings set up by MEGA.

13. REVERSIBILITY

Customer's data is retained for a 3-month period from the date of termination or expiration of the Services. During this period, Customer will no longer have access to the services. The sole purpose of this period is to allow Customer to set up a reversibility period in case of need. At the end of this 3-month period, the data are permanently erased.

Customer may request:

- Only retention of data for a period going beyond the said period of 3 months.
- Or to run reversibility services, as defined below.

Any extension of the retention period and/or reversibility services have to be received by MEGA no later than 2 months after the effective date of termination or expiration of the services.

Extension of the retention and/or reversibility services will be invoiced according to MEGA price list in forth on the date on which MEGA sends its quote to Customer.

The purpose of reversibility services is the recovery of Customer's data within the HOPEX database.

MEGA offers two types of reversibility services: basic and complex one.

- Basic Reversibility: MEGA provides Customer with backups of production data for restoration in the same version of MS-SQL-Server DBMS for a use with the same HOPEX solution in the same version.

  Data will be either (i) made available to Customer on a MEGA FTP Server for download, or (ii) sent (SFTP) on the server of Customer or its supplier. It is the sole responsibility of Customer to grant the right to access to the repository. MEGA recommends the proper training for solution administration.
- Complex Reversibility: these services are applicable where basic reversibility would not suit Customer needs. They can be appropriate when data need to be uploaded to an alternative software solution.

  The purpose of a Complex Reversibility is to provide.
  - A UTF-8 encoded XML export of the database dump;
  - A documentation on how to process XML format;
  - Acknowledged transfer of both functional and technical skills to the team in charge of the takeover, for the understanding of the data model of the solution, as well as specificities of the solution implemented, and the export provided.

  It is Customer's responsibility to approve data taken over are accurate and fully integrate within the new solution.

  Complex Reversibility shall be subject to a fixed price.
- Other: If Customer wishes to order supplemental services, it shall send MEGA its written detailed requirement. MEGA will conduct a feasibility study and/or send a quotation.

14. COMPUTATION OF TIME

When a period is stated in hours, it is computed 7 days a week and 24 hours a day.

When a period is stated in business hours, it is computed for each business day, from 9 am to 6 pm. Applicable time zone is the one for the location of MEGA's affiliate which is Customer contractor.

The time of the event or notification that causes the period to begin is not be taken into account.

When a period is stated in business days, it is computed by considering only the days of the week, from Monday to Friday, excluding public holidays applicable to MEGA's affiliate which is Customer contractor.

The day of event or notification that causes the period to begin is not be taken into account.

When a period is stated in months, it is calculated by considering the date.

The day of the event or notification that causes the period to begin is not be taken into account.

In the absence of a similar date, period is extended to the following first business day, until midnight.

When a period is stated in hours, it expires at the end of the hour.

When a period is stated in days or months, it expires at the end of the last day at 12 am.

A period stated in days that would expire on a Saturday, Sunday or public holiday is extended to the following first business day, until midnight.

Notifications by registered letter with acknowledge of receipt, shall be considered at the date of first presentation of the letter with acknowledge of receipt, the postmark as evidence.

15. MEGA’S SECURITY COMMITMENT

15.1. Global security

Subject	Description
TLS	Required on HOPEX Cloud platforms to ensure the security of transactions between the web front-end and Customer's terminal. The certificate based on TLS 1.2 AES256-SHA256 encryption is entirely at the charge of the MCS (MEGA Cloud Services) team.
Public IP whitelisting	Public IP addresses of Customers must be provided to MEGA in advance in order to access the services.
Singletenant Platform	All Customers’ platforms are fully Singletenant. Each Customers' environments are installed on a dedicated server, in a dedicated VLAN fully segregated from one other.
Virtual platforms totally segregated from each other are deployed	HOPEX Cloud platforms are typically deployed in standard mode with one virtual server per Customer for the Production environment. When subscribing to the "SaaS Platform Package" Standard or Premium level of services, three isolated instances are deployed, such as : • DEVELOPMENT: Dedicated server allowing Customer to customize HOPEX solutions and test updates; • PRE-PRODUCTION: Dedicated server synchronized on demand with the Production platform, allowing Customer to validate and test updates before their implementation in Production (e.g. Technical and functional settings, corrective patch CP); • PRODUCTION: The contents deployed on Production are previously tested and approved in the Pre-production platform.
Data encryption	Standard storage encryption from Microsoft Azure SSE using AES-256 bits encryption

15.2. Organization & Management of Information Security.

Subject	Description
Information Security organization and Information Risk Mgt	MEGA has implemented an information security policy that includes all of its personnel. The main roles of MEGA personnel are: • Senior Management approves, encourages and supports measures to improvement information system security; • The Chief Information Security Officer (CISO) is responsible for the security, availability and integrity of the information system; • The Chief Information Officer (CIO) is responsible for the operation and strategic direction of the information system; • Security Committees are formed for addressing all security topics, risks, incidents and compliance
Enterprise Risk Management	MEGA has designed and implemented an Enterprise Risks Management program to analyze and mitigate risks in a proactive way for all MEGA activities.
Independent assurance standards assessment	HOPEX Cloud Enterprise offer is subject to an annual SOC2 audit by an independent third party.

15.3. Information Security Policies.

Subject	Description
Information Systems Security Policy	This is the information system security policy that has been implemented and validated by MEGA's management and communicated to the parties concerned. This document is reviewed annually.
Procedures and policies	Information security policies (data classification, cryptography, password, etc.), standards, procedures and guidelines are published on the intranet, reviewed and communicated on an annual basis.
SOC 2 Type 2 Certification	MEGA certifies that as of the date of signature of this Agreement, the services comply with the criteria for SOC2 Type 2 certification. For sake of clarity, MEGA is not committed to maintain this compliance all along this Agreement.

15.4. Asset Management.

Subject	Description
Responsibility for assets	MEGA identifies organizational assets (Inventory, Ownership, Acceptable use and returns) and defines appropriate protection responsibilities
Information classification	MEGA implemented an appropriate set of procedures for information labeling in accordance with the information classification scheme
Media handling	MEGA has made a security policy enhancement for all CSM IT teams. No removable storage devices are allowed on the platforms.

15.5. Human Resource Security.

Subject	Description
Prior to hiring	MEGA performs necessary checks and balances on all applicants for employment in accordance with applicable laws, regulations and ethics and commensurate with the needs of the business, the classification of the information accessed and the perceived risks.
During employment	MEGA employees and external users follow a security awareness program. They receive instruction, training, and regular updates on security policies and procedures as required by their job function.
Termination and change of employment	MEGA has an HR process in place to manage any termination or change of employment.

15.6. Physical & Environmental Security.

Subject	Description
Secure areas	MEGA defined Security perimeters and Physical policy to protect areas that contain either sensitive or critical information and information processing facilities.
Equipment	MEGA has implemented physical measures to protect its equipment from unauthorized access and power outages. All storage media is scanned prior to reuse or decommissioning to ensure that sensitive data and licensed software has been securely removed or overwritten. MEGA has adopted an information security policy for workstations: protection of paper documents and removable storage media, screen lock. The HOPEX Cloud Enterprise offering is built on Microsoft Azure infrastructure, meeting a wide range of international industry-specific compliance standards such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards such as Australia IRAP, UK G-Cloud, and Singapore MTCS (https://azure.microsoft.com/en-us/support/trust-center/).

15.7. Access Control.

Subject	Description
Access Control	MEGA's global access policy is based on the principle of least privilege. Periodic reviews are conducted by the CISO (Chief Information Security Officer).
Users Access Management	The administration of the HOPEX Cloud Platforms is only accessible by the MCS team (MEGA Cloud Services) through a bastion server recording (log and video) all actions performed on Customer's platforms. The public IP address of Customer must be provided to MCS team to connect the service.
Users' responsibilities	Each Customer is granted a HOPEX Functional Administrator access which allows Customer to manage all users within the HOPEX repository. This administrator is also the contact between Customer's company and MEGA.
System and application access control	Authentication to the HOPEX Cloud service can be done through an SSO using SAML 2.0, OpenID Connect (OIDC) protocols.

15.8. Operational Security - System Security.

Subject	Description
Operational procedures and responsibilities	MCS documented all operating procedures follows ITIL Best practices (CAB) to maintain Customer's platforms in optimal conditions
Protection from malware	MEGA implemented detection, prevention, and recovery controls to protect against malware. This technical measure is combined with appropriate admins awareness.
Backup	Automatic regulars encrypted backups are performed on the HOPEX Cloud Platforms allowing to recover Customer's production data in case of incident.
Logging and monitoring	On the HOPEX Cloud Enterprise platforms, in addition to the monitoring tool HOPEX Server Supervisor embedded in all Customers' platforms allowing HOPEX Administrator to follow up every action performed on the system (e.g. Successful/Failed user authentication, User profile/rights modification etc.), all platform's logs are recorded through an MCS third-party solution for analysis. The MCS team continuously monitors each Customer's platforms availability though a dedicated monitoring system allowing to notify MCS administrators in the event of an anomaly.
Control of operational software	MCS manages the information system according to ITIL recommendations (Change management, etc.).
Technical vulnerability management	MEGA R&D uses the Coverity solution to perform vulnerability scanning on the HOPEX's source code (daily check). A third-party audit is performed on each major release. MEGA designed a vulnerability process to manage systems, software and application threats and vulnerabilities effectively and in a timely manner, mitigating the risk of potential exploitation and compromise.
Information systems audit considerations	Scheduled maintenance (OS, hardware etc.): System and software maintenances are performed during the weekend for a couple of hours. Unscheduled maintenance: HOPEX patches, customization or critical updates deployments may be performed out of the working hours and jointly planned with Customer.

15.9. Communication Security - Network Security.

Subject	Description
Network security management	All Customer platforms are dedicated (Singletenant). Each Customer platform is installed on a dedicated server isolated from each other within a separate VLAN. Each platform has its own firewall (MS Azure Network Security Group) to enforce and control network traffic.
Information transfer	Web transactions must be TLS encrypted in order to secure transactions between the web server(s) and Customer site(s). The TLS 1.2 certificate based on AES256-SHA256 encryption is fully managed by the MCS service (MEGA Cloud Services). In addition, Customer's public IP addresses must be provided to MEGA in order to join the service. This technical measure is accompanied by a data security awareness for the administrators and a confidentiality and non-disclosure agreement. In the case of a data transfer, the data must be transmitted via an SFTP type transfer.

15.10. System Acquisition, Development and Maintenance.

Subject	Description
Security requirements of information systems	MEGA delivers major versions every 18 to 24 months and minor versions are delivered every 3 months including all security patches and evolutions.
Security in development and support processes	The design of HOPEX is fully managed by MEGA. MEGA’s R&D has an SSM (Software Security Manager) in charge of: • Defining the coding best practices from a security point of view; • Reviewing all development projects specification from a security point of view; • Personally, managing the development of security-related modules (authentication etc.); • Managing campaigns of code-scans and mitigation follow-ons. MEGA does not use outsourcing development to design its solution. In case Customers need to customize its HOPEX platform (e.g. Metamodel changes), an optional HOPEX Cloud Workbench is required.
Test data	MEGA uses test database with dummy data.

15.11. Information Security aspect of Business Continuity Management.

Subject	Description
Information security continuity	The data integrity is ensured by the Geo-Redundant Storage (GRS) technology allowing to replicate backup data to a secondary datacenter which has the same security level than the primary datacenter.
Redundancies	MEGA Implemented all dispositive providing services to ensure high availability
Business Continuity Plan	MEGA designed and implemented a business Continuity Plan. 9 high level scenario which could jeopardize business continuity, along with predefined responses for optimum handling of issues.

15.12. Information Security Incident Management.

Subject	Description
Management of information security incidents and improvements	MEGA implemented Incident management process to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. This process includes an escalation procedure.

15.13. SOC 2 ADD-ON SECURITY

Subject	Description
Encryption storage	Customer’s platforms are located on encrypted storages.
CyberArk Bastion	Administrators’ sessions on Customer’s platforms are recorded though bastion