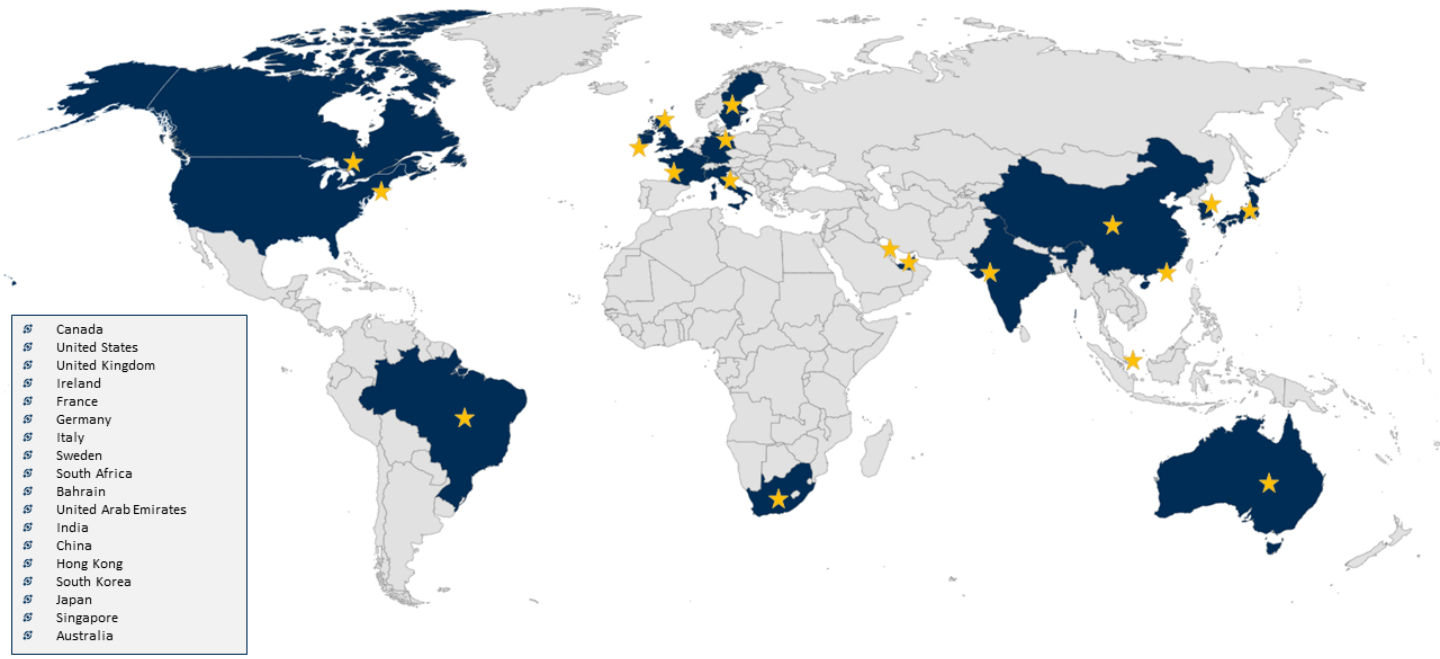
Cloud Security / Architecture

Your Data Security, Reliability, Scalability And Performance Are Critical.

Meeting high standards of security and flexibility. Interfacing's cloud solution offers you a robust technology while remaining relatively low on costs and resources. Secure data centers are located globally to ensure your location benefits from regulatory and compliance factors over and above security and performance. Keeping your data local means your services benefit from agility, reliability and support services to meet ever changing digital transformation requirements.

With the highest service standards, and the lowest network latency, efficient and rapid secure access to your data, without service interruption is our commitment to your organization. Your data is maintained on well encrypted servers and only in the location of your choice. We will never store data other than in the country of your choosing. Your browsers offer encryption when data is transferred from the servers, thereby making the connection ultimately a secure one from end-to-end.



Interfacing Cloud Security Architecture - *Global Regions

Contact us about Local On-Premise installation as well as Local Partner implementation.

Cloud Security / Architecture

SECTION	TOPIC
1	Security
2	Risk Management
3	Compliance
4	Architecture
5	SLA
6	Scalability
7	Integration
8	Training
9	Upgrades
10	Backups
11	User Authentication

Non- Functional Requirements For EPC Solution

1. SECURITY

Item	Details
Have and always maintains a ISO27001 certification.	Interfacing runs an Information Security Management System (or ISMS), program that is fully documented and certified. This program covers the entire Interfacing production line and support. In addition to our certification status, the Interfacing partner providing our cloud services (Amazon Web Services, also known as: AWS) is also certified by the ISO 27000 family series requirements (including ISO27001)
Follow OWASP development standards.	We conduct vulnerability assessments, both internally and externally. The organization's exposure to OWASP vulnerabilities are evaluated, and appropriate measures taken to address the associated risk. The QA team routinely performs penetration testing as part of their QA Plan. According to Interfacing security policies, external audited penetration tests are performing at least once per year.
Have a well-defined Information Security Policy.	As part of Interfacing's continued effort to design, implement and maintain an Information Security Management System (or ISMS). Information Security rules have been developed for the sake of outlining essential practices for protecting our information. Interfacing views information as a critical asset and therefore considers these rules to protect information availability, integrity and confidentiality. These rules inform Interfacing employees and other entities having a stake in Interfacing business of the principles governing the holding, use and disposal of information. The ISMS covers the entire scope of Interfacing processes and its organizational structure. Note: This policy document may be shared provided an NDA is in place.
Secure Library Monitoring	Automated security monitoring & alerts for any 3rd party library used within code are supported.
Secure REST API	All REST requests are using the JSON web token standard.
Encrypted data for approvals	Data is digital signature encrypted using a dynamic generated symmetric AES user private key and company public key.
Vault level AES key security Cipher strength for all signatures	Interfacing uses AWS Vault to store & manage all keys and all signatures use the AES Key Security Cipher strength for each one.
Encrypted all at rest using AES256 encryption compliant standard cipher strength	Customer data which are in rest in any form – like backup files – are securely kept on the Cloud in an encrypted form entirely using the AES256 standard.

Encrypted data in transmit is all AES256 encryption compliant standard cipher strength and supports Transparent Data Encryption (TDE)	From a database point of view, we support Transparent Data Encryption (TDE), a standard for MSSQL. The application server internal components communicate inside a private network created by the Docker engine. EPC uses the HTTPS protocol to connect to the outside world (user browser and 3rd party application). Like data in rest, EPC uses AES 256 certificate for HTTPS connections. Also, HTTPS protocol provides encrypted communication while database backup performing.
Monitoring software is in place to prevent and monitor any penetration attacks with real-time alerts and automated preventative security blocks	Interfacing utilizes Amazon GuardDuty, a threat detection service that continuously monitors for malicious or unauthorized behavior to help protect client instances and workloads. It monitors activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. GuardDuty also detects potentially compromised instances or reconnaissance by attackers. GuardDuty analyzes billions of events across Interfacing accounts for signs of risk. GuardDuty identifies suspected attackers through integrated threat intelligence feeds and uses machine learning to detect anomalies in the account and workload activity. When a potential threat is detected, the service delivers a detailed security alert to the GuardDuty console and AWS CloudWatch Events.
Has a registered DPO that oversees all client data actions	Interfacing has a data protection officer (DPO), who is responsible for reporting any breaches. No employee except the Data Protection Officer (DPO) and authorized support agent (on request with approval) can access, wipe or delete the client's database. ISO 27001 certified Interfacing ISMS legislations support corresponding procedures. Our cloud-hosting provider, AWS, has robust procedures for responding to an IT security breach as well. These include, Breach containment and preliminary assessments, Evaluation of the risks, notification of the breach, and Investigation of the breach. Each of Interfacing's SaaS customers have their servers on AWS separately with separate backup folders and unique keys for data transmission encryption. Except for Interfacing support managers, no one has access to customer's cloud machines (and as mentioned before, they have no rights/permissions to edit, copy or delete the databases and require the intervention of the DPO to conduct such procedures (based on customer request/authorization).
Block and log attack patterns, such as SQL injection or cross-site scripting	Interfacing conducts regular penetration tests, both internally and externally. Information about technical vulnerabilities obtains in a timely fashion (quarterly). The organization's exposure to such vulnerabilities evaluated and appropriate measures and actions taken to address the associated risk. The QA team routinely performs penetration testing as part of their QA Plan. According to Interfacing security policies, external penetration tests are performed at least once per year. Type of tests include: -Bypassing authentication test using the SQL injection method -XSS Tests using Stored and Reflected XSS besides DOM-based XSS -CSRF Tests Vulnerability Tests Validation for User Level Impact -Bypass Authentication Using Back Browser Button -User input Tests Client-Side change data. -User Input Tests HTML Injections -Test Session for Page Content Validation using no Redirect Add on -Access and Control Tests using different permission mechanisms -Bypass Authentication using SQL Injection (brute force method) - Login Page
Conduct Vulnerability & Threat detection testing every 3 months at a minimum.	Interfacing conducts regular vulnerability assessment and penetration tests, both internally and externally. This includes information about technical vulnerabilities obtained by internal vulnerability assessments that are performed in a timely fashion (quarterly). The organization's exposure to such vulnerabilities are evaluated and appropriate measures and actions taken to address the associated risk. The QA team routinely performs penetration testing as part of their QA Plan. According to Interfacing security policies, external penetration tests are performed at least once a year.

Log all audit changes to any content in the system	An audit trail is a chronological set of records that provide documentary evidence of the sequence of activities that have affected an EPC object at any point in time. It concerns itself with who did what, when where and how. The EPC records modifications made to objects, and as such, allows users to download audit trails in the form of an excel spreadsheet.
Log all administration changes in application and in hardware platform (what, who, when, where)	The Administrator's Operations logging process reports user activities (Cloud Administrators, exceptions, faults and information security events) within client's cloud resources. Interfacing keeps these logs safe and are regularly reviewed. The report may contain the following information if relevant: · User IDs · Activity · Time Stamp · Asset identity (Hardware, Software, etc.) · Event Type .Access attempt .Configuration Change .Error or Exception (descriptive)
Retain all logs for 90 days	Interfacing maintains all logs for 10 years.
Vunerability code scanning & conduct code review before any commit	Interfacing R&D uses the IntelliJ IDEA (Source code scanning tool). Also, the IntelliJ inspections and Sonar Lint plug-in are utilized during programming (real-time scanning). https://rules.sonarsource.com/ http://www.jetbrains.com/idea/features/ On top of these tools, the QA teams code reviews 2 levels of reviews on every code commit inside our development team performs routinely. The R&D team also has automated testing at the API level and supporting backend, front end, UI animation and UAT testing. We can also track all libraries that used, can be flagged for security alerts, and fixed to update to the latest code level.
Virtual Private Cloud to provision a logically isolated section of the cloud environment to launch instances in a virtual network	Interfacing provides a dedicated Virtual Environment for Enterprise customers, including separated EC2 Instances, separated VPC with segregated subnets for frontend, backend and database server, and separation between production and testing environments in different VPCs. We leverage the approach described below to successfully meet the security outcomes equivalent to physical separation through logical separation, as required for DoD IL5. Virtual Private Cloud (VPC) — The EPC solution for Enterprise client's provision in a logically isolated section of the AWS Cloud, where the client's AWS resources reside in a virtual network that we define. The VPC strictly enforce access and security restrictions between your web servers, application servers, and databases. The VPC provides advanced security features to enable inbound and outbound filtering at the instance level and subnet level, restrict access so that it's only accessible from instances within your VPC. Sufficient demonstration that VPC creates the equivalent of entirely separate network domains for each tenant;
Segregate all customer databases (not multi-tenant)	Interfacing provides a dedicated Virtual Environment for Enterprise customers, including: • Separated EC2 Instances (Web application Server) • Separated database servers • Separated VPC (Virtual Private Cloud) with segregated subnets for frontend and backend upon customer request (extra charges may apply) • The separation between production and testing environments in different VPCs

Complete segregation of production and non-product network environment	Virtual Private Cloud (VPC) — The EPC solution for Enterprise client's provision is in a logically isolated section of the AWS Cloud, where the client's resources reside in a virtual network that we define. The VPC strictly enforce access and security restrictions between your web servers, application servers, and databases. The VPC provides advanced security features to enable inbound and outbound filtering at the instance level and subnet level, restrict access so that it's only accessible from instances within your VPC. Sufficient demonstration that VPC creates the equivalent of entirely separate network domains for each tenant.
Web application specific firewall that helps protect against application availability, compromise security, or consume excessive resources.	Interfacing is using a web application firewall (WAF) for each in-production server. The WAF helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. WAF gives us control over which traffic to allow or block to your EPC instance by defining customizable web security rules. Custom rules block common attack patterns, such as SQL injection or cross-site scripting. Hence, Interfacing cloud administrators can define certain rules that are designed for your specific application.
Information Security Program	Interfacing runs an ISMS program that is fully documented and certified. This program covers all Interfacing production lines and support. Additionally, AWS is also certified by ISO 27000. Interfacing extends its ISMS program scope as much as possible. This verified scope document includes almost every aspect (e.g. Software, Hardware, Network, Data), which are related to customers or other stakeholder's data directly or indirectly. The program follows ISO 27000 guidelines, and in doing so, follows the PDCA concept. Interfacing ISMS covers the following titles as verified implementation for its Cyber Security program. -Planning -Asset Management -Risk Management -Compliance -Controls Selection and Implementation -Threats and Vulnerabilities Assessment and Treatment -Monitoring and Reporting -Incident Management -Event Analysis -Recovery Plans -Management Reviews -Documentation and Communication -ISMS Continual Improvement
Documented Incident Management Process	Interfacing uses a documented process for Incident Management not only for internal security incidents but also for cloud (production environment) incidents. Interfacing uses different implementation for cloud services than internal ones, although the concept of the process is the same. In the event of a security-relevant incident, an incident analysis will be completed, including cause & effect (including diagnostics of customers data) and corrective and preventive action plans put into place to ensure such an incident does not re-occur. Interfacing will communicate to your team the root cause of the incident, any impact (if any) on your data, corrective actions taken to control the situation and quickly restore a seamless working environment, any potentially harmful effects associated with the incident and preventive steps taken to ensure no recurrence of the event.

Monitoring and Reporting procedure for critical assets and production environments	**On-Premise Assets:** Interfacing uses monitoring tools for monitoring critical assets. There is a process for reporting abnormal events for further investigation and driving the risk management process. **Cloud Assets:** On the cloud, by using AWS CloudTrail and AWS CloudWatch, all cloud resources events and activities are logged and continuously monitored. Also, relevant alerts and notifications notify the IT and support team. **Instance Monitoring:** The client's instance is hosted on the cloud (AWS), and the Interfacing support team uses a cloud monitoring tool (AWS CloudWatch) for cloud resources, starting with the instance. It provides visibility into resource utilization, operational performance, and overall demand patterns— including metrics such as CPU utilization, disk reads and writes, and network traffic. In addition, CloudWatch is set up with alarms to notify the support team if certain thresholds are crossed, or to take other automated actions such as adding or removing instances if Auto-Scaling was enabled. CloudWatch also captures and summarizes utilization metrics natively for AWS resources.
Perform the background verification process for all human resources.	"Interfacing Onboarding Process" has a mandatory step for running an independent background verification per each employment candidate. Only when receiving a "clear" status will the process go forward on the potential employee's candidacy.
The approach toward PII and Not PII information	**Personal Identification Information** The EPC application does not store any highly sensitive personal information/data such as Credit Card, Bank Account details or similar personal data. The entire EPC database will be stored on the cloud(AWS) cloud infrastructure only, which is fully secure and capable of providing high availability for business continuity. No data storage is outsourced or stored on third-party support apart from AWS. In the case of a migration project of client data, the Interfacing service team will work on a dedicated Amazon instance in a separated secured subnet on the same AWS account as the client's servers are. The specialized machines for our service team are configured according to the least permission concept. No data is copied to Interfacing onsite infrastructure. **Non-Personal Identification Information** We may collect non-personal identification information about SaaS users whenever they interact with an instance. Non-personal identification information may include the browser name, the type of computer and technical information about Visitors means of connection to the instance, such as the operating system and the Internet service providers utilized and other similar information which help Interfacing R&D and Support team to make the SaaS as optimized as possible.
Encryption Keys shall be managed via a secure key management system.	AWS Key Management Service (KMS) is used to create and manage keys and control the use of encryption across a wide range of AWS services. AWS KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules to protect keys. AWS KMS is integrated with AWS CloudTrail to provide logs of all key usage to help meet regulatory and compliance needs. KMS is fully managed. Administrator control access to encrypted data by defining permissions to use keys while AWS KMS enforces permissions and handles the keys durability and physical security.

All REST requests use the JSON web token standard	JSON Web Token is considered an open standard that defines a compact and self-contained way for transmitting information between parties as a JSON object in a secure manner. This information can be verified and trusted because it is digitally signed. EPC uses this technology while transferring the JSON objects between its internal components.
Centralize all logs across application & ability push to logs to a corporate central 3rd party log management tool	Interfacing uses Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, and other sources. CloudWatch Logs enable us to centralize the logs from all of our systems, applications, and AWS services that we use, in a single, highly scalable service. At any time, administrators can view them, search them for specific error codes or patterns, filter them based on particular fields, or archive them securely for future analysis. CloudWatch Logs enable us to see all of our cloud infrastructure logs, regardless of their source, as a single and consistent flow of events ordered by time, and can be queried, sort based on other dimensions, group by specific fields, create custom computations with a powerful query language and visualize log data in dashboards. Also, the cloud notification service makes Interfacing clients capable of pushing these logs to other systems via varied methods like emails, JSON objects and SMS. Apart from records, AWS CloudWatch allows Interfacing to monitor production environments in a real-time manner automatically and notify the support team instantly. The following metrics are subjected to real-time monitoring by default: • Instance Availability • CUP usage • Free Disk Space

2. RISK MANAGEMENT

Risk Management Process	Interfacing performs Risk management in compliance with ISO 27001, which drives the ISMS forward. Various processes like vulnerability assessment, systems like incident management systems and authorities like the support team are responsible for feeding the Interfacing Risk Management Process. This depends on risk evaluation outcome, relevant authorities (DPO, IT Manager or ISMS Committee) who decide about the most effective controls to treat the risk. Interfacing Quality Management System (QMS) also aids this process for proper documentation and communication. QMS, which is a customized instance of EPC, holds all threats, vulnerabilities and risks caused that are detected. Reports which are generated by this tool help Interfacing, the security team and management to treat risks properly.

Frequent Internal and External Audit performs to conclude Information Security Management System established, implemented, maintain and continually improve	**Audits** Interfacing ISMS schedules quarterly internal audits. Also, as an ISO 27000 certified company, Interfacing has to be audited independently once per year. **Internal Audit** The internal audit activity helps an organization fulfill its security objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes. **External (Independent) Audit** The corresponding report will be disclosed provided an NDA agreement is signed.
Ready for being audited by the client (Customer Audit)	Interfacing is ready to accommodate against meeting the following requirements: • Written notice in advance (60 Days) • Signed NDA
Ready for being audited by the client (Vulnerability Assessment and Penetration Test)	Interfacing is ready to accommodate against meeting following requirements: • Written notice in advance (60 Days) • Signed NDA

Cloud Architecture for Medium Size Businesses	For the medium-size client, EPC comes with an All-in-One deployment. This type of client-server implementation includes the application server, database server and reporting server installed in a single windows server cloud instance (AWS EC2). The instance also has secure connections to two other cloud services. For the sake of safe storage of backups, the instance has a link to the cloud storage service (AWS 3 Bucket). Also, the cloud mail service (AWS SES) is responsible for sending out emails that are ordered by EPC. Many options are available to add to the architecture based on customer requirements (which does not include in the figure). The following list includes some of these options which may use in the deployment: -Integration with Local and Cloud ADFS Server -Load Balancing -Auto Scaling -Virtual Private Cloud -Detail Monitoring by using advanced AWS CloudWatch metrics -Continues Threat Detection by using AWS GuardDuty -Automated security assessment by using AWS Inspector -Hardware security module (HSM) to generate and use encryption keys on the AWS Cloud -Long term backup solution -Automatically discover, classify, and protect sensitive data by using ML & AI algorithms * Using one or a combination of the above services may result in extra charges.

Communicate downtimes in advance	**EPC Downtime (Planned Downtime)** For the sake of third-party software updates, EPC upgrade or maintenance activities, downtime will be scheduled with advanced notification for EPC SaaS activities. Interfacing will run these maintenance activities during an agreed-upon period that minimizes any potential downtime for the customer. **Cloud Services Downtime (Planned Downtime)** AWS may schedule events for instances, such as a reboot, stop/start, or retirement, which do not occur frequently. If the instance will be affected by a scheduled event, AWS sends an email to the email address that's associated with the corresponded AWS account before the planned event. The email provides details about the event, including the start and end date. Depending on the event, the administrator might be able to take action to control the timing of the event and communicate with the corresponding client's site administrator.
99.99% uptime Guarantee	**SERVICE COMMITMENT** Interfacing will use commercially reasonable efforts to make Interfacing EPC Cloud available with a Monthly Uptime Percentage (defined below) of at least 99.99%, in each case during any monthly billing cycle (the “Service Commitment”). In the event Interfacing EPC Cloud does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below. **SERVICE COMMITMENTS AND SERVICE CREDITS** Service Credits are calculated as a percentage of the total charges paid by you (excluding one-time payments such as upfront payments) for EPC Cloud in the Region affected for the monthly billing cycle in which the Region Unavailability occurred in accordance with the schedule below. Monthly Uptime Percentage Service Credit Percentage Less than 99.99% but equal to or greater than 99.0% 10% Less than 99.0% 20% If ever there were to be a service uptime interruption of five (5) or more consecutive days, Interfacing will credit client a 100% of that month’s fees and client will have the right to immediate contract termination. Interfacing will apply any Service Credits only against future EPC Cloud payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the Unavailability occurred. Service Credits will not entitle you to any refund or other payment from Interfacing. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the Interfacing Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide EPC Cloud is the receipt of a Service Credit (if eligible) in accordance with the terms of the SLA.
RPO: 4hours / RTO: 4hours	Default Interfacing SaaS configurations are supporting 30 minutes RTO and 4 hours for RPO. Upon customer requirements, greater RPO and RTO times are available (these may be subject to extra charges). Interfacing uses MSSQL on the instance, which provides real-time replication of DBs within multiple locations. Additionally, we also take VM snapshots every 24hours. Amazon Web Services are available in multiple regions around the globe (e.g., America’s, EMEA, and the Asia Pacific). We choose the most appropriate location for the Disaster Recovery (DR) site, in addition to the site, where the system is fully deployed. Amazon EBS provides the ability to create point-in-time snapshots of data volumes or an instance. The snapshots store in Amazon S3. Amazon EBS volumes provide off-instance storage that persists independently from the life of an instance and is replicated across multiple servers in an Availability Zone to prevent the loss of data from the failure of any single component.

6. SCALABILITY

Support Load Balancing, & Auto-Scaling across multiple servers	**Load Balancing** Load Balancing automatically distributes incoming application traffic across multiple instances. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones. Load Balancing offers three types of load balancers that all feature the high availability, automatic scaling, and robust security necessary to make your applications fault-tolerant. Against none functional requirement analysis that performs by Interfacing BAs and BSAs, one or more than one of the following types of load balancing may use. These configurations may cause extra charges. **Auto Scaling** Auto Scaling monitors servers and automatically adjusts the capacity to maintain steady, predictable performance. The service lets us build scaling plans for resources, including EPC instances, associated databases and reporting servers.
Stateless user session management (no sticky sessions)	In EPC, the client session is stored with the client. In this architecture, there is no session affinity or sticky sessions. The relevant session information is stored with the client and passed to the server as needed. In alignment with user management best practices, EPC client's application state will never be stored on the server-side. By using this practice, EPC is capable of scaling thousands of concurrent users.
File stream persistence (Scalability for large file management: stream video/images/docs/rich text)	EPC is using File Stream technology to handle considerable size files persistence. This technology is useful when the solution is dealing with objects that are being stored are, on average, more significant than 1 MB. On the other hand, EPC users experiencing faster read access, which is vital for enterprises.

Micro Service Architecture	EPC's internal blocks communication entirely relies on REST API technology. In addition, EPC uses Rest API for integration with other environments. The list below shows a shortlist of tasks that could perform in EPC via APIs. The detailed specification is communicated with the customer representative before the end of the deployment phase. -Approval Cycle Management -Objects Comparison -Collaboration on EPC objects -EPC object CRUD -User Management - Bulk User Import and User Synchronization -SOP / Books Generation -Authentication, Authorization -EPC Administration -Information Import/Export -Search within the environment
All product functions and features available within an open and secure REST API (including multi-lang updates)	EPC uses Rest API not only for interconnection but also for integration with other environments. The list below shows a shortlist of tasks that could be performed in EPC via APIs. The detailed specification will be communicated with the customer representative before the end of the deployment phase. -Approval Cycle Management -Objects Comparison -Collaboration on EPC objects -EPC object CRUD -User Management - Bulk User Import and User Synchronization -SOP / Books Generation -Authentication, Authorization -EPC Administration -Information Import/Export -Search within the environment
Well Documented API	The EPC APIs detailed specification will be communicated with the customer representative before the end of the deployment phase. This comprehensive specification document includes Methods, Actions, Input, Output and Examples for each EPC API. EPC administrators can use this document as a guide for making integration between EPC and other applications.

8. TRAINING

Provide access to all soft copies of training materials for reuse. Create and provide videos of all new features for each release for continuous learning	Whenever there is a new release, Interfacing sends a newsletter to all clients describing the objective of the release, including details and screenshots of all new features and bug fixes as well as an invitation to attend a Free "What's New in version X" webinar. This webinar is open only to customers and describes all new functionalities in detail. Customers also have access to the webinar and all other soft copy training materials for further use. For significant enhancements or new features, additional training can be provided either through on-premise/online training sessions or training videos. Details of each release are also always available directly online within Interfacing's online HELP and posted within Interfacing's customer support portal as well. For broader communications, Interfacing uses general email announcements, blogs, posts using Social Media such as LinkedIn, newsletters, webinars, trade shows, etc. Additionally, your dedicated account executive communicates releases via physical visits, personally made phone or video calls and emails.

9. UPGRADES

Notify and request upgrade before applying any upgrades	You have access to Updates and Upgrades upon their release. Updates and Upgrades including: (i) fixes to critical and other issues reported and discovered in the Services, (ii) enhancements and modifications for better functionality of the Service. Interfacing support team consults the single point contact from the administration side of those customers who are using Interfacing single-tenant deployments in advance of upgrade performance. The value of our cloud environment is that we ensure it is our responsibility to upgrade your environment, therefore allowing you to remain on the latest version instead of waiting on local IT support. There is no capital expenditure (CAPEX) on Software License and Hardware required or request support from your internal IT group for resolving issues or request an upgrade to the latest release. Typically, we have two major releases (upgrades with significant function and features enhancements) and four minor releases (modifications, fixes, smaller improvements to existing features) per year.
Automation testing of every REST API call & scenario	We have automated testing at the API level, which supports backend automation rest level, front end UI animation testing and UAT testing. We can also track all libraries that are used, and can be flagged for security alerts, and fixed to auto-update to the latest code level.
Upgrades: Database versioning with automated migration (ensures no corruption)	Our team creates and tests all migration scripts to ensure a smooth and seamless upgrade from one version to the next without any loss of data. This ensures its easy for clients to stay on the latest version which includes all the latest security standards.

10. BACKUPS

Take real-time incremental backups	Interfacing SaaS customers have automated backups of their database instance storing in secure cloud storage (Amazon S3). DB backups are taken every four hours and can be more frequent upon client request (e.g., real-time.).
Take full database backups at least every 4 hours	Interfacing performs a backup every four hours as our Backup Process lowest service level standard.
Take full VM snapshots of application, API and database applications at least every 24 hours	Interfacing backs up the customer instances' data to cloud storage by taking point-in-time snapshots daily. Snapshots are incremental backups, which means that only the data blocks on the device that have changed after your most recent snapshot are saved. The incremental snapshot minimizes the time required to create the snapshot. Each snapshot contains all information needed to restore the instance (from the moment when the snapshot was taken). When an instance volume based on a snapshot was created, the new volume begins as a replica of the original volume that was used to create the snapshot. The replicated volume loads data in the background so that it can be used immediately.
Retain all backups for a minimum of 90days	Backup files retainment cycle: 90 Days Interfacing provides 90 days of retainment cycle for all backup files as the lowest level of service standard. Upon customer request, the retainment cycle can be extended (extra charges may apply).

11. USER AUTHENTICATION

SAML 2 ADFS & AZURE Single Sign-on Support	EPC supports the following protocols for user authentication. According to customer need, the Interfacing deployment team will help customers to choose and configure the most proper authentication system. • SAML 2.0 • Kerberos • LDAP Authentication • NTLM • Azure Single Sign-On
Support Just-in-Time user creation	When a user goes to access the system (when the client has SSO configured with Just-in-time), the system will authenticate them at point of access and then automatically create users on-the-fly. This allows the client not to have to pre-sync the users but instead have them added automatically to the system on-demand

Cloud Security / Architecture

End of Document