Skillsoft Cloud Operation Services

Revision History

Date	Version	Description	Author
1/12/2007	1.0	Description of the CO Services Operations	Cloud Ops
1/16/2007	1.1	Topology Diagrams and Security Attestation added	Cloud Ops
3/14/2007	1.2	The company logo changed	Cloud Ops
4/15/2008	1.3	Updates to backup, app description, load balancing, capacity planning, remote access, antivirus, wireless access in the office.	Cloud Ops
10/3/2011	1.4	Modification of backup process	Cloud Ops
12/15/2011	2.0	Password encryption modification, Laptop and mobile devices security, Wireless security, Data transfer security, Database cleansing, Employee background check, TrustE, Company Insurance, Skillsoft's Privacy Policy	Cloud Ops, HR, Legal, IT
3/5/2013	3.0	New Disaster Recovery Process, Vendors: Iron Mountain, Job Titles modifications	Cloud Ops
12/23/2013	4.0	Minor updates: SSL, TrustE, SSAE 16	Cloud Ops
2/18/2015	5.0	Deprecation of SSL v3. FedRAMP certification, Akamai Upgrade, Java -Free offering	Cloud Ops
1/4/2017	5.1	TrustE and Safe Harbor and Privacy Shield changes, FedRAMP status update	Cloud Ops
5/16/2017	5.2	Iron Mountain data center description and FedRAMP authorization	Cloud Ops

Introduction

Skillsoft offers its eLearning solutions under the Software as a Service (SaaS) model. SaaS alleviates the complexities involved in managing a web applications that have to be accessible over the Internet on a 24/7 basis. SaaS provides several advantages, among them, the removal of the burden placed on an organization's IT resources to manage and administer yet another Web application.

With the SaaS solution our customers' IT Management no longer needs to worry about:

- Hardware costs
- Software Licensing costs
- Application monitoring
- Creation of in-house expertise to support the eLearning solution
- Dealing with application and content upgrades
- Allocation of IT staffing to perform recurring maintenance
- Security management for the application
- Management of Desktop configurations
- Backup/Restore management
- Augmentation of helpdesk staffing

Skillsoft Cloud Operations (CO) have developed policies and processes to ensure application performance while maintaining the highest security standards. Following is the description of these processes and the overall CO Services provided by Skillsoft. For companies that are restricting the extrnal IP addresses that can be accessed from within the company, Skillsoft will provide a range of IP addresses that will have to be open for the Skillsoft application to work properly. More information on the IP ranges can be provided by the Account Team that supports the customer account or Skillsoft Technical Support.

Privacy

Due to the E.U. Parlament decision to overturn the Safe Harbor Privacy Principles on October 24th, 2015, Skillsoft offers currently Model Clause agreements to its E.U. customers.

Skillsoft is committed to data privacy and is compliant with the existing EU Data Protection Directive as enshrined in applicable local EU member state law, such as the UK Data Protection Act 1998. Skillsoft will

be implementing data protection measures and processes to ensure compliance with the General Data Protection Regulation (GDPR) prior to it coming into force on 25 May 2018. As a company, we are taking all necessary steps during the two-year transition period, which commenced on 27 April 2016 to ensure compliance by 25 May 2018.

Privacy Shield

Skillsoft has already started the process of evaluating its current practices and procedures to determine what changes need to be made to meet the new statutory obligations for data processors under the GDPR. A roadmap specific to Skillsoft's operations has been drafted by our external privacy counsel to guide us through identifying the areas that require changes to compliant with the GDPR. We are now developing a plan based on this roadmap to help ensure that all required changes are implemented by the time the new regulation takes effect.

As part of this process, we will implement the appropriate technical and organizational measures to ensure personal data is protected. Our contracts will adhere to the stricter requirements that will be in place for contracts between data controllers and data processors. To meet the new accountability requirements for data processors, we will maintain written records regarding our data processing activities. Skillsoft's Data Protection Officers will monitor company compliance with the GDPR. We will also ensure that our internal procedures account for the new data breach notification obligations under the GDPR.

Given the significant changes the GDPR imposes on data processors, we expect it will take some time to implement the actions and processes necessary for compliance, but we are fully committed to being in compliance with the GDPR before it becomes effective on 25 May 2018.

In addition, Skillsoft intends to pursue Privacy Shield certification this year. We engaged external privacy counsel to perform a comprehensive assessment of Skillsoft's relevant business processes, EU personal data collection and use practices, and personal data flows from the EU to the US to evaluate our privacy policies and practices against the Privacy Shield Framework requirements. Once this process is complete and any necessary modifications have been made to our policies and procedures, Skillsoft will seek Privacy Shield Self-Certification with the US Department of Commerce.

We are committed to completing this review and self-certification process as soon as reasonably practicable so that we can use Privacy Shield as a transfer mechanism to comply with EU data protection requirements. In the meantime, Skillsoft is happy to enter Standard Contractual Clauses to govern such transfers.

Skillport Application Description

Skillport is a JSP application using Tomcat services, with a proprietary Java LMS (Application Server) . The application uses a SQL database to store various configuration parameters as well as student credentials

and student progress records. Each SaaS customer has a dedicated application and database instance. A number of Skillport applications share the same hardware pool, however the customers are completely isolated from one another.

From a user perspective, the application is accessible via a Web browser on port 443. Courses launch via a 'Content Player', written in HTML 5. Customer's site will be configured run via HTTPS. By default the site will be configured TLS 1.0 or higher.

Load Balancing

All current generation products achieve maximum scalability and service availability through a classic hardware load-balanced architecture. All real-time application level components provide both horizontal and vertical scalability options that are constantly monitored against key performance criteria and are appropriately scaled on demand. Core infrastructure component are implemented in either an active-active, or active-passive failover model.

Data Center and Co-Location Services

Skillsoft owns and manages a Private Cloud infrastructure for its SaaS application. For its data centers Skillsoft contracts co-location services with Tier 1 service providers, SunGard and Iron Mountain. SunGard facility in Aurora, Colorado is the primary facility that hosts Skillsoft Private Cloud and its SaaS applications. The Iron Mountain facility in Northborough, MA is a disaster recovery hot site. SunGard and Iron Mountain data centers provide redundant high-bandwidth connectivity and scalability enabling Skillsoft to develop its Private Cloud service rapidly and effectively. Security access includes multiple levels of physical and digital access controls. Both SunGard and Iron Mountain delivers highly reliable network connectivity and state-of-the-art collocation facilities providing the best possible operating environment to Skillsoft's customers.

The SunGard and Iron Mountain data centers includes VESDA fire detection and FM-200 fire surppression. A 2N redundant power supply provides dual power feeds and backup batteries, water coolant systems, and generators. An N + 1 redundant climate control system provides primary and backup chiller units, cooling towers, and water storage. Additionally, a local network operations center (NOC) monitors the data center's operations continuously. Physical access to SunGard and Iron Mountain data centers is kept secure by 24x7 guards with interior and exterior closed-circuit television surveillance, electronic access at all data center entrances, including electronic key management systems and individually keyed cabinets and cages.

SunGard is **SSAE16 Type II SOC 2** Certified. Certification is available upon request.

Iron Mountain facility is **SSAE16 Type II SOC2 and SOC3** certified, **FISMA** certified, **ISO27001** certified, **PCI DSS Level 1** certified and **HIPAA** certified

Additional information about SunGard and Iron Mountain data centers and co-location services can be obtained from SunGard and Iron Mountain directly.

Network Device Control

Description of the network, routers, switches, firewalls

Recognizing the critical nature of network and security infrastructures Skillsoft has made strategic investments in best-of-breed devices from vendors such as Cisco and F5 Networks reflecting our ongoing commitment to world-class service provision. Network infrastructures are built for scalability and fault resilience following many of the guidances used by Internet Service providers.

Perimeter security is provided through a robust Firewall and Intrusion Detection and Prevention system. This multi-vendor, multi-layer system affords customers the greatest degree of protection from Denial of Service attacks and intrusion attempts while positioning Skillsoft to respond with agility to emergent threats.

All systems are built from standardized, pre-hardened images employing industry best-practices. System images are routinely reviewed to ensure responsiveness to a changing technology and threat landscape.

As a final measure Skillsoft conducts an annual, third-party security audit of our Private Cloud Environment. Skillsoft has enjoyed a very favorable asessment history with no high-risk vulnerabilities found during its assessments.

Control Program Management

Restart and recovery procedures

A comprehensive monitoring infrastructure ensures that Skillsoft CO personnel are alerted at the earliest opportunity of service affecting conditions. Clearly articulated governances inform the assigned CO Engineer what actions are permitted without escalation and specific details on how prescribed actions

should be undertaken. In the event that a condition arises for which there is no defined procedure, the issue is escalated to a CO manger for consideration.

Restriction on system access

Respecting the confidential nature of the data entrusted to Skillsoft by our customers and in an effort to provide the most stable Private Cloud Environment possible, privileged access to all SaaS application infrastructure is restricted to CO Personnel only. Under no condition is system access granted to any party outside of CO Services with the exception of service providors under a direct support or professional services contract with Skillsoft.

System documentation

Extensive documentation has been created covering all aspects of system construction, application installation and product configuration and management. These documents are constantly updated to reflect the most current policies and procedures. All documents remain under strict version control and any changes are subject to multi-party reviewed and approved.

Protection from unauthorized access

Privileged access to all Skillsoft CO entity is strictly controlled and available only to CO personnel. Under no circumstance is access granted to non-CO personnel to any system. Strict and consistently enforced protocols ensure that all access is immediately suspended following any job action affecting CO personnel.

Data Protection Procedures

Overall backup strategy

Skillsoft CO Services has invested in a multifaceted backup strategy that blends the best features of traditional tape, block-based disk copies and secondary disk storage.

Backup schedule for application data

In order to ensure the greatest possible flexibility and speed-of-recovery minimal primary data is stored on application servers. Application data is stored off-site on an independent disk infrastructure which is accessible to the SaaS Infrastructure with minimal latency. In cases where primary data exists on application systems, this data is relocated to a central disk repository and committed to tape each night.

Backup schedule for databases

Database data files are backed up using two separate but complimentary methods. The first is a block-based disk copy to a set of independent disk on the storage array which enables CO Services to conduct complete data file backups of all databases every three hours. Because of the light-weight and fast nature of this operation it can also be done ad-hoc in advance of scheduled maintenance activities to ensure point-in-time recovery to a pre-maintenance state. Additionally, data is committed to tape each night.

Backup schedule for log files

All pertinent log files are automatically relocated to a centralized disk library each night and retained there indefinitely. They are additionally committed to tape on a nightly basis.

Backup Encryption

For all SQL backups CO uses FIPS 140-2 compliant software encryption option within BackupExec, which allow for a 256-bit AES pass phrase, which must be at least 16 characters. In our case, we are actually using a randomly generated 64-character string.

Backup Details

All of the following backups are accomplished using Backup Exec 11d at the current time. The backup server uses LTO3 media.

1. Skillsoft performs SQL full snapshots to disk every 3 hours.
2. Skillsoft performs SQL full backups to tape every night.
3. Skillsoft backs up all Admin servers and storage each night.
4. Product and Customer Specific files are replicated and put to tape each night.
5. Replicated copy of content is kept on another storage unit for quick recovery.

Backup Schedule

Skillsoft utilizes a combination of full and differential backups using disk-based and LTO tape media to provide flexible and comprehensive customer data protection. The specific backup routines vary depending on the nature of the data being retained and are as follows:

- Skillport Database backups – Full backups are committed to tape nightly (Mon, Tues, Wed, Thurs, Fri, Sat and Sun).

- Administrative servers are backed up with nightly differentials and monthly full backups.

- Product and customer specific files are backed up with a customized differential and full back up schedule.

- Network Attached Storage (NAS) – NAS data is committed to tape via NDMP backups with customized full and differential backup schedules. NAS data includes all course and Dialogue content as well as various customer-specific assets such as logos and graphics.

Backup Rotation

- Tapes are collected from the data center every Wednesday and secured in a third-party off-site facility; tapes are moved back into rotation once data has expired.

- Skillport Database daily full backups are retained onsite for 3 months in disk based storage unit (Virtual Tape Library).

- Skillport Database weekly full backups are retained onsite for 6 months in a disk-based storage unit (Virtual Tape Library) and LTO tape media are retained for 1 month at an offsite 3rd party storage facility.

- Skillport Database monthly full LTO tape media backups are kept at an offsite 3rd party storage facility for 36 months.

- Skillport Database yearly LTO tape media backups are kept at an offsite 3rd party storage facility for 60 months.

- Administrative server differential backups are stored on disk-based storage unit (Virtual Tape Library) for 3 months and monthly full backups to LTO tape media are stored at an offsite 3rd party storage facility for 36 months.

- Product and customer specific backups are retained onsite in the disk-based storage unit (Virtual Tape Library) per CO data retention requirements defined in internal documentation.

Monthly full backups to LTO tape media are retained at an offsite 3rd party storage facility. Product and customer specific data on LTO tape media is set to never expire.

NAS backups are retained onsite in the disk-based storage unit (Virtual Tape Library) per CO defined data retention requirements defined in internal documentation.

Offsite storage

Skillsoft CO Services has contracted a third-party (Iron Mountain) to recover and store all tapes at a secure, remote facility. This partnership is governed by an aggressive SLA that ensures that Skillsoft CO Services is able to restore services to customers at the earliest opportunity and minimize any service disruptions.

Time to recover the various types of backup

Depending on the nature of the fault and the historical requirements of the data recovery times will vary. Recovery of data from a block-based disk backup and full restoration of service is expected to be complete within 60 minutes of initiation. Recovery and restore of historical data from a remote facility including full service restoration is expected to compete within 8 hours.

Outages Management

The SaaS applications are broadly monitored for availability from multiple physical locations. Visual and auditory alerts are generated within 1 minute of a service fault and email alerts generated within 2 minutes. Immediate action is undertaken to restore impaired services. All service affecting events are logged and analyzed by both SW Engineering and CO resources to ensure that the event is fully understood and steps are taken to mitigate future exposure to the event.

Slowness in Applications Performance

In addition to tracking the availability of Hosted services, comprehensive measures are in place to protect against subtle or transient application latency. A redundant and geographically dispersed monitoring infrastructure provides visual, auditory and email notification for any monitoring event that surpasses the allowable time limit. The transactional monitors emulate user activity and provide a reliable indicator of general end-user system performance.

Security Breach Management

In the event that SaaS application or services are compromised Skillsoft CO Services would immediately implement an environment lock-down blocking all inbound and outbound communication from the datacenter environment. Privileged remote connectivity would be maintained for CO Security and Network Personnel to ensure the timeliest resolution of the issue. Every effort would be taken to close the breach, re-stabilize the systems and limit exposure of customer data. A detailed post-mortem of the events would be conducted at the earliest opportunity and shared with our customers as appropriate.

Process for communicating back to customers

Communications to the customer are effected through the Learning Consultants with root cause analyses available to customers upon request.

Overall uptime report provided on an ongoing basis

Customers can elect to have monthly reports provided detailing system response time and availability on a monthly basis. The reports will be sent automatically at the beginning of the month showing uptime and response time for the previous month.

Systems Recovery from a Service Affecting Event

Hardware Failure

Many systems in the Private Cloud Environment are hardware load balanced and the loss of a system is not service affecting. In cases where hardware redundancy is not provided, fully configured, hot-standby systems are available for immediate use. Recovery policies and procedures are documented to enable quick response to such incidents restroing services quickly and efficiently.

Application Malfunction

Application faults are detected through continuous system monitoring and mean time to resolution in generally less than 10 minutes. Procedures for corrective actions are documented and all application faults are escalated to SW Engineering for investigation.

Network Loss

A fully redundant network infrastructure enables Skillsoft to provide the most highly available infrastructure possible. Redundancy is provided at all levels including the Internet connection. Failover tests are conducted on a regular basis to ensure that configuration modifications and patch installations did not effect the reliability of our fault tolerance.

Impaired Application Performance (i.e latency)

Application latency is detected through continuous system monitoring and mean time to resolution is generally less than 10 minutes. Procedures for corrective actions are documented and all application latency events are escalated to SW Engineering for investigation.

Trusted Recovery

In the event that a third party needs to be involved in a system recovery, the third-party engagement will be subject to formal contract terms which are reviewed and refined by the Skillsoft legal team before engagement. Third-parties directly handling sensitive information are subject to and bound by Non-Disclosure Agreements.

Virus Protection

System level virus protection and prevention is afford by a centralized virus management system. This centralized system facilitates a rapid response to emergent threats and ensure a uniform posture across all Private Cloud Infrastructure.

Skillsoft uses Symantec Antivirus Enterprise Edition utilizing the automatic update engine, which makes available to systems protection from all known virus signatures. Vendors that work on the premises with their own laptops are subject to virus scan and virus update by Skillsoft's IT department prior to connecting to Skillsoft's network.

Frequency of Signature Updates

Virus signature updates are reviewed and deployed on a continuous basis in response to emergent threats. CO maintains a very tight schedule for antivirus updates maintaing the both the application and the virus signatures up to date.

Disaster Recovery

To facilitate the most rapid recovery possible, Skillsoft CO Services has a documented Disaster Recovery Plan that details the responsible parties, the communication protocol and the steps that will be taken in the event of a disaster. Skillsoft has a redundant site located in Northborough, MA. The redundant site is

at a distance of, 1900 miles from the primary Private Cloud site, located in Aurora, CO. The Aurora site is managed and owned by SunGard Recovery Services; the site in Northborough is owned and managed by Iron Mountain. The two facilities are setup in an active-active configuration, with a target RPO of 180 minutes and a target RTO of 12 hours.

The Primary and the D.R. sites are linked via a dedicated 10GB line replicating customer data between the two sites on a continuous basis. The replication uses a disk block-based replication technology. Additionally, disk-based backup devices in Aurora are continuously replicated to a redundant device in Northborough. Skillport applications are configured to use a native, vendor-supplied virtual machine recovery suite, which provides rapid and fully automated recovery of the infrastructure to the remote facility.

Skillsoft conducts an annual D.R. test staging a failover of a sample of its SaaS applications and infrastrcture. D.R. test results are available to customers upon request.

Compliance with Standard Architecture

All production systems are deployed using best of breed security practices. All systems are in essence replicas of a master Image making the deployment process efficient and speeding recovery time following an unrecoverable system fault. As best practices change so does the image used as the master.

All operating systems are loaded with the most current updates from the OEM. This is done using a suite of externally and internally developed tools.

All systems are harden to limit unauthorized Admin or Super User access using industry and vendor best practices including:

- Complex naming and password standards
- User access control settings
- Redirection to disabled accounts.

All systems are checked to insure that any unnecessary or potentially exploitable services are set to be disabled at power on. Some of these services are:

- Alerter
- Clipbook Viewer
- Computer Browser
- Distributed File System
- Distributed Link Tracking Client

- Distributed Link Tracking Server
- Error Reporting Service
- Fax Service
- Help and Support
- IMAPI CD-Burning COM Service
- ICF/ICS
- Indexing Service
- Intersite Messaging
- Kerberos Key Distribution Center
- License Logging Service
- Messenger
- NetMeeting Remote Desktop Sharing
- Network DDE
- Network DDE DSDM
- Print Spooler
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Remote desktop Help Sessions Manager
- Smart Card
- Smart Card Helper
- Telnet
- Uninterruptible Power Supply
- Utility Manager

Change Management – Roles and Responsibilities

Technology managers have defined approval boundaries and act as an approving authority for adjustments that are contained to their area of purview. Changes that have a wider impact are submitted for multiparty consideration of all stakeholders. Stakeholders considering change requests are as follows:

- Network and Security Manager
- Application Services Manager
- Database Manager
- Storage and SANS Manager
- Cloud Operations Director
- Global Cloud Operations – SVP

The Cloud Operations Direcotr and Clobal Cloud Operations SVP have final veto authority on all change requests.

System Configuration – Management

Adjustments to system images or configurations are strictly controlled through a multi-party review and approval process involving Management, Network and Security, System Architects and System Engineering resources. Documentation is immediately adjusted in response to system reconfiguration.

Change Process, Testing and Approval Process

Change requests are submitted by the initiating party to the appropriate technology manager for initial consideration. The area manager will then invoke guidance of the CO Director to determine the scope of the change and establish an approval roster. Whenever possible changes are vetted through advanced implementation in a staging environment and in some cases warrant and receive load testing by a dedicated automation team.

To ensure the quality of work, changes to the environment are verified by CO Supervisors on an ongoing basis. The CO Architects conduct physical audits quarterly to ensure that the environment meets the defined standards.

Configuration and Security Specification

Skillsoft employs a “most-restrictive” policy in regards to all network device policies and access controls. Firewall, IDP and IDS rules are continually reviewed and monitored for suspicious events. Device configuration is standardized and heavily documented. Adjustments to configurations and policies are reflected in the associated system or device documentation.

Configuration Control

Adjustments to any device by a network technician require the approval of the Network Manager and in some cases will additionally require the CO Director approval. An adjustment to any aspect of host system configuration requires the review and approval of the Senior System Architect and in some cases the CO Director. All configuration adjustments or changes are reflected in the associated system or device documentation.

Security, Accounts and Password Management

Password Management

Generic Usernames and Passwords use is discouraged wherever possible. Administrators are granted individualized logins and empowered to manage their own passwords according to the domain enforced password policy

Password Expiry

All user account Passwords are scheduled to expire every 30 days. Passwords must meet strict complexity requirements and cannot be reused. Paswords history are managed via GPO.

Password Length and Complexity

Passwords must meet a minimum character and complexity requirements including a minimum character restriction as well as requiring non-alphanumeric characters and characters of mixed case. Passwords length and complexity are managed via GPO.

Password Protection

Efforts are made to limit the communication of passwords to verbal channels and passwords are provided on a need-to-know basis. When verbal communication of passwords is not possible, username and password combinations are communicated in separate correspondences and only to the target audience. Sharing of user account passwords is strictly prohibited.

Physical Security Description

All Skillsoft SaaS applications are located in a third-party SSAE 16 compliant facility providing 7x24 access control to a defined access control roster. The facility employs multilayered access control governances including mantrap doors, CCT, card-only access and 7x24 guards. Premises are unmarked.

Environment – Security Description

A multi-tiered perimeter defense infrastructure ensures the greatest possible protection from unauthorized access or malicious activities. Measures include a most-restrictive firewall policy, network and pattern-matching intrusion detection and prevention systems as well as an extensive and current anti-virus infrastructure.

Systems – Security Description

All systems are constructed from standardized, pre-hardened images using industry best practices in accordance with Skillsoft specific system and software requirements. Routine and ongoing patch management is controlled via centralized patch management software ensuring a consistent and current posture.

Personnel – Security Management

Employee actions (hiring, terminations, suspensions, etc.) are fully coordinated with Human Resources and corporate IT providing immediate and coordinated responses to all CO personnel status changes. Additionally, CO management is apprised of all Skillsoft staff terminations should special measures be required to protect against actions of ex-employees with privileged knowledge or understanding of Skillsoft proprietary software and/or infrastructure.

Employee Laptops and Mobile devices encryption

Skillsoft utilizes file-level encryption strategy leveraging software that seamlessly encrypts files at rest and in transit based on risk-levels, as defined in the information policy. The risk-factor is determined as a combination of content, context and type of data. All customer data is defined as sensitive information and treated accordingly. For data that can potentially be copied via auxiliary devices such as USB thumb drives, CD and DVD, The IT department rolled out an Enterprise Information Protection software that will detect and prevent Skillsoft's employees from transferring customer sensitive information via mobile devices (i.e., CD-RW/DVD-RW, USB, flash drives, PDAs, cameras, mobile phones).

Access to the Hosted Environment

All privileged access and communication to the Private Cloud environment is secured through either client or site-to-site encryption. Site-to-site tunnels providing privileged port or service access are restricted to Skillsoft CO-Only subnets. Remote access authentication is tightly integrated with existing domain security and provides for a single point of administration. Remote access is restricted to CO personnel. This policy is universal and comprehensive to include administration, backups, etc. Under no

circumstances is privileged access afforded to SW Engineers, Learning Consultants, Application Engineers, corporate IT or Account Executives.

Remote Access to the Hosted Environment

The production system can be accessed only by the CO Engineers. Access to the various subsystems is segregated based on duties and responsibilities. Each engineer has a unique user ID and password that is managed via an ACL that grants access only to the systems that are under the engineer's area responsibility. Since most CO engineers need access to the Private Cloud environment 24/7, they have laptops however the laptops have only the operating system and VPN software on it. To access the Private Cloud environment the CO engineers connect remotely from their laptop to their desktop machine on Skillsoft premises, which has the VPN software that provides connectivity to the Private Cloud environment. The access is authenticated via a two-factor authentication from RSA Security. Application passwords are changed every 30 days or when an individual in CO leaves their job role.

Third Party Annual Penetration Test

In a continuing effort to improve the security of the Hosted environment, Skillsoft contracts a third-party security organization to conduct an annually full penetration and vulnerability assessment of the Private Cloud Environment. This assessment reviews Firewall policies, Intrusion Detection and Prevention policies, System patch levels, vulnerability to known software exploits and brute force attacks. Assesment results are available to customers upon request.

Vendor, Technology and Platform Disclosure

As a countermeasure to intelligence gathering, Skillsoft will not release to customers under any condition the make, model or manufacturer of any network or security device in use within the Private Cloud Environment. This includes release of information related to:

- Firewall related hardware/software/settings
- Intrusion Detection System related hardware/software/settings
- Network penetration testing
- Vulnerability scanning
- Network topology
- Internal IP scheme
- Operating Systems configuration and security settings
- Software vendors and version used.

System Maintenance

Description of planned system maintenance schedule

Skillsoft currently provides for 2 weekly routine maintenance windows. They are as follows;

- Wednesday: 1 AM – 2 AM ET
- Sunday: 1 PM – 3 PM ET

Activities conducted in these maintenance windows may include, but is not restricted to, hardware maintenance and replacement, system patching, infrastructure enhancements and Skillsoft software releases.

Customers located in the Asia Pacific region, have the option to elect an alternate Wednesday maintenance window. This option should be discussed with Skillsoft Learning Consultant assigned to the customer account.

Emergency Maintenance

Skillsoft reserves the right to conduct unplanned maintenance activities when a delay of said maintenance is seen to pose a significant risk to the availability and or security of the services provided. Every effort is made to coordinate these unscheduled maintenance activities with clients in advance and to conduct these activities at the least impactful time as circumstances allow for.

Maintenance Schedule

All scheduled maintenance window activities are coordinated and planned in advance with established cut-off windows. All activities are critically examined to ensure timing and that all activities are non-overlapping.

Security Management

Maintenance activities are restricted exclusively to CO personnel and access is strictly governed through multipart security measures.

Wireless in the office

Skillsoft provides to its employees wireless access within Skillsoft premises. The wireless service uses WPA2 Enterprise encryption for access to Skillsoft network environments. All wireless access requires unique authentication and is logged to a central location which is reviewed for failed access attempts. Rogue wireless detection is performed continuously to prevent malicious activity.

Access points are configured to utilize Radius Authentication. A unique secure SSID is configured. Wireless traffic is secured and managed via firewall Policies. Allowed ports are limited to HTTP (80), HTTPS (443) and VPN Ports (TCP/UDP).

Wireless access is segregated via its own Ethernet interface on Skillsoft's Firewall with no access to internal corporate resources. VPN must be utilized to gain access to corporate resources.

Production Code – Change Control

Product Development

Product related software development is done by Skillsoft SW Engineering staff, which consists of System Architects, Application Engineers and Database Developers. The SW Engineering department is divided by the various areas of expertise required by the various products and their respective SW Engineering life cycle.

QA Processes

A dedicated Quality Control team ensures all software made available to customers is of the highest quality and performance. This team has final veto authority for all software packages moving to production systems.

Qualification Processes

An extensive and comprehensive testing matrix is applied to all Skillport software releases testing functionality and support for a wide variety operating systems and browser versions. New functionality is tested extensively and existing functionality is additionally tested to safeguard against regressions.

Software Rollout into Production

Following a formal release to Skillsoft CO Services the software release package is reviewed by CO Services and a deployment strategy is assessed. Software then enters a controlled release cycle initially deployed to a small, pre-determined number of systems. Following this 7 day controlled release, a

general release cycle is undertaken with all systems receiving the update over a series of scheduled maintenance windows.

Patch Management and Version Management

Continuous improvements to software occasionally result in patches being available to Skillsoft software product lines. All major and minor software releases including patches are uniquely versioned and this version in transparent to all operators. The release strategy for patch deployments models that of the general software release process described above.

SW Engineering – Change Control

SW Engineering Process

Following the finalization of functional specifications, general software architecture is determined by the product software Architect and a CO Services Architect In some cases Architectural considerations may result in changes to functional specifications. These adjustments are communicated back to the respective stakeholders and a final functional specification and architecture is determined. This architecture is documented and released to the SW Engineering manager for review, project scoping and resource assignment.

Access to Source Code

All software access and versioning is strictly controlled through a software source control package. Access to source code is provded on an as-needed basis and is exclusively restricted to Skillsoft SW Engineering.

Software Release Process

Authority to release software from SW Engineering to QA is restricted to the SW Engineering manager responsible for the product line. Authority to release software from QA systems to final qualification systems is restricted to the assigned Quality Control Engineer provided the software has meet the pre-defined acceptance criteria for release. Authority to release software from final qualification to Skillsoft CO Services is restricted to the assigned Quality Control Engineer (with QA Manager assent) provided the software has meet the pre-defined acceptance criteria for general release.

Patch Management – Process Description

Software

A centralized patch management software suite ensures a consistent security posture across all managed systems and empowers Skillsoft CO Services to aggressively respond to emergent threats. All available software patches are considered by CO Architects and deployed on a schedule in accordance with the associated risk.

Security and Network Devices

A dedicated team of network and security professionals continuously consider newly available patches and enhancements to network and security devices. Signature bundles for IDP and IDS devices are downloaded daily and considered for implementation on a continuous basis.

Account Controls

Access to Systems

Access to all Private Cloud Systems is restricted to Skillsoft CO Services personnel. In select cases Vendor-authorized technicians are afforded access to the systems in conjunction with hardware failure events or professional services engagements.

Access Management

System and Facility access control is governed by a select body of Skillsoft CO Services personnel. System access is granted at a level commensurate with job function. Access to security and network devices is restricted to the Network Management team, the CO Director and the Senior CO Architect. Data center facility access is managed in conjunction with the collocation service provider through a formal ACL. Governance of this ACL is restricted to CO Managers.

Boundary Defenses

Firewalls

Skillsoft has selected best-of-breed hardware and software solutions from established industry leaders. Firewalls utilize a most-restrictive policy providing only for known and require port access. Access to firewalling systems is strictly controlled and adjustments to any firewall policies is subject to managerial approval prior to implementation

Intrusion Detection Prevention (IDP)

Through granular pattern matching and event correlation Skillsoft provides comprehensive protection against known vulnerabilities and zero-day defense against emergent threats. IDP signatures are considered and updated on a continuous basis.

Intrusion Detection System (IDS)

A redundant, active IPS implementation provides effective and proven protection against brute force and denial of service attacks. Adjustments to the IDS configuration are considered on a continuous basis.

Secure data transmission

All client-server communications and data exchange is protected by 128 bit encryption provided by a recognized Certificate Authority. In certain scenarios customers elect to provide user data directly to Skillsoft for direct insertion into Skillsoft Hosted applications. Skillsoft provides a SecureFTP transfer for this service.

Connection to the Public Internet and SSO

Skillport services are available through the public internet however measures exist to ensure unauthorized access to your Skillsoft services does not occur. This includes username/password-only access to your Skillport site and empowering customers to perform their own application account management in accordance with their own policies. Skillsoft also offers Single Sign On (SSO) options to enable customers to validate their users via the customer internal authentication mechanism and obtain seamless access into Skillsoft SaaS applications.

Audit Trail Protection

Logs Management

Aggressive system logging captures all events relating to system access including privileged user right use, service stops/starts, logins, and logouts. Firewall and network intelligence logs capture all failed access events and suspicious activities as defined by our IDP/IDS infrastructure. Comprehensive sysloging and SANS/Storage management logging capture all non-standard events. Detailed application logs trap all unusual application events in addition to verbose web server logs. All system, security and access logs are retained by Skillsoft CO Services for an indefinite period. All event logs are archived daily to centralized disk storage for convenient access. This centralized repository is then committed to tape and retained according to our tape retention policies as defined in this document. Access to logs is restricted to CO personnel with the exception of application error and web logs which are shared with Skillsoft SW Engineering on an as-needed basis.

Data Retention and Protection

Customers' Data - Storage

All customer data is stored on an enterprise storage array providing the maximum degree of data protect and integrity available. Customer data is stored exclusively in relational databases with no data present on Internet-facing web systems. Access to this data is restricted to CO personnel and only duplicated to tape format. In some cases customer data is duplicated into a secured and controlled lab environment for the purposes of issue resolution or capacity planning exercises directly relating to the customer. Customer data is stored in a database specific to the customer.

Customers' Data - Protection

Access to database systems and customer databases is restricted to CO personnel only. Privileged remote access is exclusively conducted over a secure, encrypted channel. Tape backups are entrusted to a leading authority in data and tape storage with the media stored at a remote, secured facility and accessible only to a restricted group within the CO Services organization.

Data Encryption

Customers' user account password are encrypted in their respective database using a SHA 256 hashing algorithm.

End- User Access Methods

All data access occurs through publicly accessible, password protected web systems. Direct data access is never afforded.

Data Availability Following Contract Termination

Customers can export their data from Skillsoft SaaS applications at any time uisng the Company Admin privileges via the Reporting interface.

Personnel management

Roles and Responsibilities

Skillsoft has assembled a world-class team of IT professions around an organizational structure that provides clear lines of accountability, oversight and ownership without sacrificing agility and responsiveness to customers. The CO Services team is generally divided into the following teams:

- Networking and Security
- System Architects
- Application and Systems Administrators
- Database and SANS Administrators
- Product Support and Provisioning
- Program Management

Employee Background Checks

Skillsoft recognizes the sensitivity of the data handled by the CO employees. To ensure the best security awarness and due dilligence, Skillsoft performs background checks (subject to applicable local laws) with respect to pre-determined positions that require access to customer data. Skillsoft also checks references provided by candidates generally as part of the application process. Additionally all CO employees are required to review and sign a Security and Privacy Policy that details roles and responsibilities, escalation procedures and overall code of conduct with the CO organizations. All CO employees are required to sign the policy annually acknowledging their understanding and commitment to its guidelines.

Dedicated CO Team

Skillsoft recognizes the unique challenges facing Service Providers and the specialized skill sets required to effectively manage and grow Private Cloud infrastructure. In direct response to this, Skillsoft has heavily invested in a dedicated CO Services team whose sole mandate is to ensure the best possible experience for our Hosted customers.

Expertise Description

Skillsoft CO Services boasts a seasoned and skilled team of technology professionals. In addition to years of industry tenure, many CO Services personnel also carry industry certifications including certifications from the following authorities;

- Cisco
- Microsoft
- CheckPoint
- Hewlett Packard
- GIAC
- FedRAMP
- VMWare
- EMC
- CommVault

Personnel Training

In an ever changing and evolving technology landscape, Skillsoft recognizes the critical role training plays in the successful delivery of services. To ensure that Skillsoft has the best possible resources available to its customers, Skillsoft aggressively pursues training for all products resident in the Private Cloud Infrastructure. This included a formal training agenda for proprietary products developed by Skillsoft.

Capacity Management

Skillsoft takes project management very seriously to ensure that capacity is available for new products, new customers, customers' upgrades and systems replacement. The Skillport application and its add-ons are subject to load testing validating the hardware requirements and the deployment configuration.

The Skillport application and its add-ons are deployed based on a pre-defined deployment plan that maps out exactly how many Skillport applications will share the same hardware pool and, how will the

hardware pool be configured. The required hardware is pre-built and configured based on build sheets and pre-configured images that were created by the system analysts. The existing hosted environment is continuously monitored for resource utilization. Since emergency situations may arise, the CO department has 'standby' inventory ready to be deployed to address any capacity issues that may arise.

Third Party Service Providers

Cachefly

Skillsoft uses Cachefly to improve content delivery performance in the EMEA and APAC regions. The Cachefly service is used to expedite the course delivery to the end user. The application and the student progress tracking is done by Skillsoft within the Skillsoft SaaS application.

Verizon Media

Skillsoft also uses verizon streaming services (previously known as EdgeCast). The streaming service iis used for video streaming that is delivered from the Books24x7 platform.

Iron Mountain

Skillsoft uses iron Mountain for its offiste backups storage. Iron Mountain is responsible for the secure transport and storage of the backup media.

FedRAMP Certification

Federal Risk and Authorization Program (FedRAMP) is an intiative by DoD and Federal Government to standardize Cloud Services selection and audits for DoD and Federal Customers. The FedRAMP is founded on NIST 800-53 /rev. 4. Under FedRAMP mandate, Skillsoft currently conducts monthly system and application scans, reported to agencies that are subject to FedRAMP compliance. Skillsoft also conducts a FedRAMP annual security audit conducted by an indepndent third party. **Skillsoft is FedRAMP Authorized**.

Information regarding Skillsoft's FedRAMP authorization can be found at:

https://marketplace.fedramp.gov/#/product/private-cloud?status=Compliant&sort=productName

Appendix B – Skillport Topology

Hosting Environment Network Topology