Skillsoft Cloud Operations (CO) Services
Percipio Hosted in the E.U

Revision History

Date	Version	Description	Author
3/27/2019	1.0	Description of the Cloud Operations and the Private Cloud in the E.U.	Cloud Ops.

Introduction

Skillsoft offers Percipio via the Software as a Service (SaaS) Model. Percipio is accessible via the web alleviating the complexities involved in managing a web application that has to be accessible over the Internet worldwide, 24/7/365.

The SaaS model 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
- 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 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 Percipio application to work properly. More information on the IP ranges can be provided by the Account Team that supports the customer account.

Privacy Shield / GDPR

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 implemented data protection measures and processes to ensure compliance with the General Data Protection Regulation (GDPR).

Skillsoft rolled out a tool from TrustArc to inventory all applications that store E.U. users' Personal Identifiable information. Skillsoft also developed tools that enable its customers to exercise the right to be forgotten for a user.

In addition, Skillsoft pursues 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. A Model Clause agreement is available for Skillsoft E.U. customers.

Percipio Application Description

Percipio is a web application developed on Micro Services architecture. The application uses RedHat's Open Shift platform, Docker containers, Kubernetes, Kafka, PostgressSQL databases, Casandra database for reporting and analytics and other technologies that are best-of-breed in the Micro Services Architecture. The Percipio application uses Java and Ruby at its core. The application uses the SQL database to store various configuration parameters as well as student credentials and student progress records. Customers are segregated in the SQL database by an organizaion key unique to each organizaion.

Percipio application uses Multi-tenancy by unique identifier. All Customers use the same database and schema, but the rows of the table have a unique OrgID which is used in retrieving data for an Organization. Within an Organization there is a unique UserID which is used (in certain cases) to further filter the data to a single user.)

The unique identifiers are generated using the UUID v4 format (https://en.wikipedia.org/wiki/Universally_unique_identifier) – These identifier are randomly generated by software libraries complying with RFC4122 (https://tools.ietf.org/html/rfc4122#section-4.1.3).
The chances of guessing one of them is next to zero (https://stackoverflow.com/questions/4878359/what-is-the-probability-of-guessing-matching-a-guid)

PII and other user data

The application stores in its SQL database user data:

- First Name,
- Last Name and
- email address.

- Activity, such as access to courses, books, audiobooks
- Time spent on Channel and Course Pages
- Collection level consumption
- Assignment status

For users/learners, the application is accessible via a Web browser on port 443. Courses launch via the HTML5 JWPlayer.

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 and are constantly monitored against key performance criteria and are appropriately scaled on demand. Core infrastructure components are implemented in either an active-active, or active-passive failover model.

Data Center and Co-Location Services

Skillsoft contracts data center and co-location services with Tier 3+ service provider, British Telecom (BT). The location of the data center is in Frankfurt, Germany. BT data centers provide redundant high-bandwidth connectivity and scalability enabling Skillsoft to develop its hosting service rapidly and effectively. Security access includes multiple levels of physical and digital access controls. BT delivers highly reliable network connectivity and state-of-the-art collocation facilities providing the best possible operating environment to Skillsoft and its customers.

The BT data center 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. BT achieved a Power Effectiveness Wert (PUE) of 1.3. Physical access to BT data center 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. The facility has a perimeter fence with a entrance gate remotely controlled and monitored via CCTV by BT security personnel.

BT data centers have the follwing certifications:

ISO 9001 – Quality Management

ISO 20000 – IT Process, ITIL

ISO 27001 – Security Management

ISO 14001 – Green IT

Additional information about BT centers and co-location services can be obtained from BT 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 CO Environment. Skillsoft has enjoyed a very favorable asessment history with no high-risk vulnerabilities found during any 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 conditions arises for which there is no defined procedure, the issue is escalated to a manger immediately.

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 CO environment possible, privileged access to all Private Cloud systems is restricted to CO personnel only. Under no condition is system access granted to any party outside of CO with the exception of service providers under a direct support or professional services contract with Skillsoft. No Third Party Service providers have access to customers' data.

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 review and approval.

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

System backups are not meant for the following purposes:

- Data Archival
- To safeguard against scenarios not directly related to the loss of data

The data backup is accomplished using CommVault Simpana, consists of two stages:

- Disk backup – Utilizing disk-based storage array to store backups at the hosting facility, making them available for quick restore if necessary. The backups will be the recent data backups
- Tape Backup – Utilizing backup LTO6 media. The tapes are encrypted using FIPS 140-2 compliant software encryption option within the backup platform, which allows for a 256-bit AES pass phrase that must be at least 16 characters. Skillsoft will utilize a randomly generated 64-character string.

Backup Schedule

Systems will be backed up according to the schedule below:

Information Class	Frequency/Type	On Disk Retention	Offsite Retention	Comment
Percipio Relational Databases	Daily	90 Days	N/A	**Predominantly customer application data**
	Weekly	90 Days	90 Days	
Network Attached Storage	Daily	90 Days	N/A	**Includes administrative, repositories and application data sets**
	Weekly	90 Days	90 Days	

Backup Media Retirement

Media will be retired and disposed of as described in the Skillsoft Digital Asset Destruction Policy.

Prior to retirement and disposal, Global Cloud Operations will ensure that:

- The media no longer contains active backup images
- The media's current or former contents cannot be read or recovered by an unauthorized party.

Backup Verification

On a daily basis, logged information generated from each backup job will be reviewed by the backup administrator for the following purposes:

- To check for and correct errors.
- To monitor the duration of the backup job.
- To optimize backup performance where possible.
- IT will identify problems and take corrective action to reduce any risks associated with failed backups.
- Random test restores will be done once a week in or der to verify that backups have been successful

Hosting will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

Data Recovery

In the event of a catastrophic system failure, off-site backed up data will be made available to users within 3 working days if the destroyed equipment has been replaced by that time.

In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 working day.

Restoration Requests

In the event of accidental deletion or corruption of information, requests for restoration will be made via Skillsoft Tech Support. A ticket will be opened by Skillsoft Tech Support assigning the restoration request to Global Cloud Operations - Hosting Support.

Incident Management

All Private Cloud Systems 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 the Private Cloud 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 the Private Cloud systems or services are compromised Skillsoft CO 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 Skillsoft Tech Support and Learning Consultants with root cause analyses available to customers upon request.

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 do 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 unlikely 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.

Disaster Recovery

To facilitate the most rapid recovery possible, Skillsoft Hosting 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 hosting site located in the U.S. in Northborough, MA. The Disaster Recovery data center is managed by Iron Mountain. The redundant site is at a distance of, over 5000 miles from the primary hosting site, located in Frankfurt, Germany. In the event of a disaster, customers will be given the option to redeploy the Skillsoft SaaS products in the U.S. Customers sites will be redeployed after obtaining written approval from our customers. Skillsoft is currently developing a Disaster Recovery Plan that will keep the data in the E.U. The plan is to have the D.R. plan completed by the end of 2019.

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.

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 hardened 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 ensure that any unnecessary or potentially exploitable services are set to be disabled at power on.

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 – S.V.P.

The Cloud Operations Director and Global Cloud Operations S.V.P. 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 Analysts 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 engineer require the approval of the Network Manager and in some cases will additionally require the CO Director’s 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 are forbiden. 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. Password expiry are enforced via GPOs.

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. Password length and complexity are managed via GPOs.

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 Private Cloud systems are located in a third-party ISO 27001 compliant facility providing 7/24 access control to a defined access control roster. The facility employs multilayered access control governances including mantrap doors, CCTV, card-only access and 7/24 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 require to protect against actions of ex-employees with privileged knowledge or understanding of Skillsoft proprietary software.

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 Private Cloud 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 Private Cloud-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 developers, Learning Consultants, Application Engineers, corporate IT or Account Executives.

Remote Access to the Private Cloud Environment

The Private Cloud systems 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 of 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 Private Cloud environment, Skillsoft contracts third-party security organizations to conduct annually, full penetration and vulnerability assessment of the Private Cloud Environment. Thess assessments review 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.

Planned System Maintenance

Description of planned system maintenance schedule

Routine maintenance window operations (when service-impacting) are restricted to two hours per week. Special maintenance windows of longer duration may be requested from time-to-time for which 14 days advanced notice will be provided.

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.

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 Scrum Masters, DevOps Managers, Squad Architect, SW Engineers and Database Developers. The SW Engineering department is divided into Squads by the various areas of expertise required by the various products and their respective software development 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 Percipio sprints testing functionality and support for all technologies listed in the product compatibility matrix. 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 staging environment. Following qualification in the staging environment, the software package is deployed in production. The Micro Services architecture enables SW deployment quickly and seamlessly.

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 DevOps Architect assigned to each squad. 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 DevOps manager for review, project scoping and resource assignment.

Access to Source Code

All software access and versioning is strictly controlled through Github, 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 DevOps 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 commensurating with job function. Access to security and network devices is restricted to the Network Management team, the CO Director and the Senior CO Architect. The Private Cloud Facility access is managed in conjunction with the colocation 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 traffic 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 Prevention System (IPS)

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

Connection to the Public Internet

Percipio SaaS application is available through the public Internet however measures exist to ensure unauthorized access to the SaaS applicaiton do not occur. This includes username/password-only access to your Percipio site and empowering customers to perform their own application account management in accordance with their own policies via the Learning Administrator interface. Customer can elect to implement Single Sign On (SSO) ensuring better protection and ease of use for its users.

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.

Report to customers regarding a security violation incident

Skillsoft follows a strict Incident Management process approved by its DoD and Federal customers. If a security incident occurs. Information related to the incident will be provided via Skillsoft's Tech Support team to the customer's primary contact. The first phase of the contact will acknowledge that a problem occurred and the status of the remediation. Subsequent updates will be sent during the remediation process. Once the incident was addressed CO will conduct a root cause analysis and the results will be provided to customers upon the customers' request.

Data Retention and Protection

Customers' Data - Storage

All customer data is stored on an enterprise storage array providing the maximum degree of data protection 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. Customer data is duplicated to the Private Cloud Disaster Recovery site, which is also strictly managed by CO team. Customer data is backed up daily and transferred securely on encrypted tapes to an offiste facility managed by Iron Mountain. 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. Duplicated data used in the lab environment is subject to database scrubbing, which removes all customer Personal Identifiable Information (PII) from the data prior to its use in the lab. To ensure the data security and privacy, the scrubbing process occurs within the Private Cloud environment prior to exporting the data into the lab.

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 (Iron Mountain) 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.

Password Storage

Customers' user account password are hashed (and salted) securely using bcrypt

End- User Access Methods

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

Personnel management

Roles and Responsibilities

Skillsoft has assembled a world-class team of IT professionals 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 Data Storage Administrators
- Product Support and Customer 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 within the CO organization. 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 Cloud infrastructures. 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 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
- RedHat
- DevOps
- CheckPoint
- EMC
- GIAC
- VMWare
- CommVault
- AWS Cloud Practitioner

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 and generic security / privacy courses assigned to employees annually.

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 Percipio application is subject to load testing validating the hardware requirements and the deployment configuration is meeting our customers' demand.

The Percipio application is deployed based on a pre-defined deployment plan that maps out exactly how the Percipio application shares the hardware and, how will the hardware be configured. The required infrastructure is pre-built and configured based on build sheets and pre-configured images that were created by the system

architects. The existing Private Cloud environment is continuously monitored for resource utilization. Since emergency situations may arise, the CO team has redundant capacity ready to be deployed via configuration, to address any capacity issues that may arise.

Third Party Service Providers

Fastly

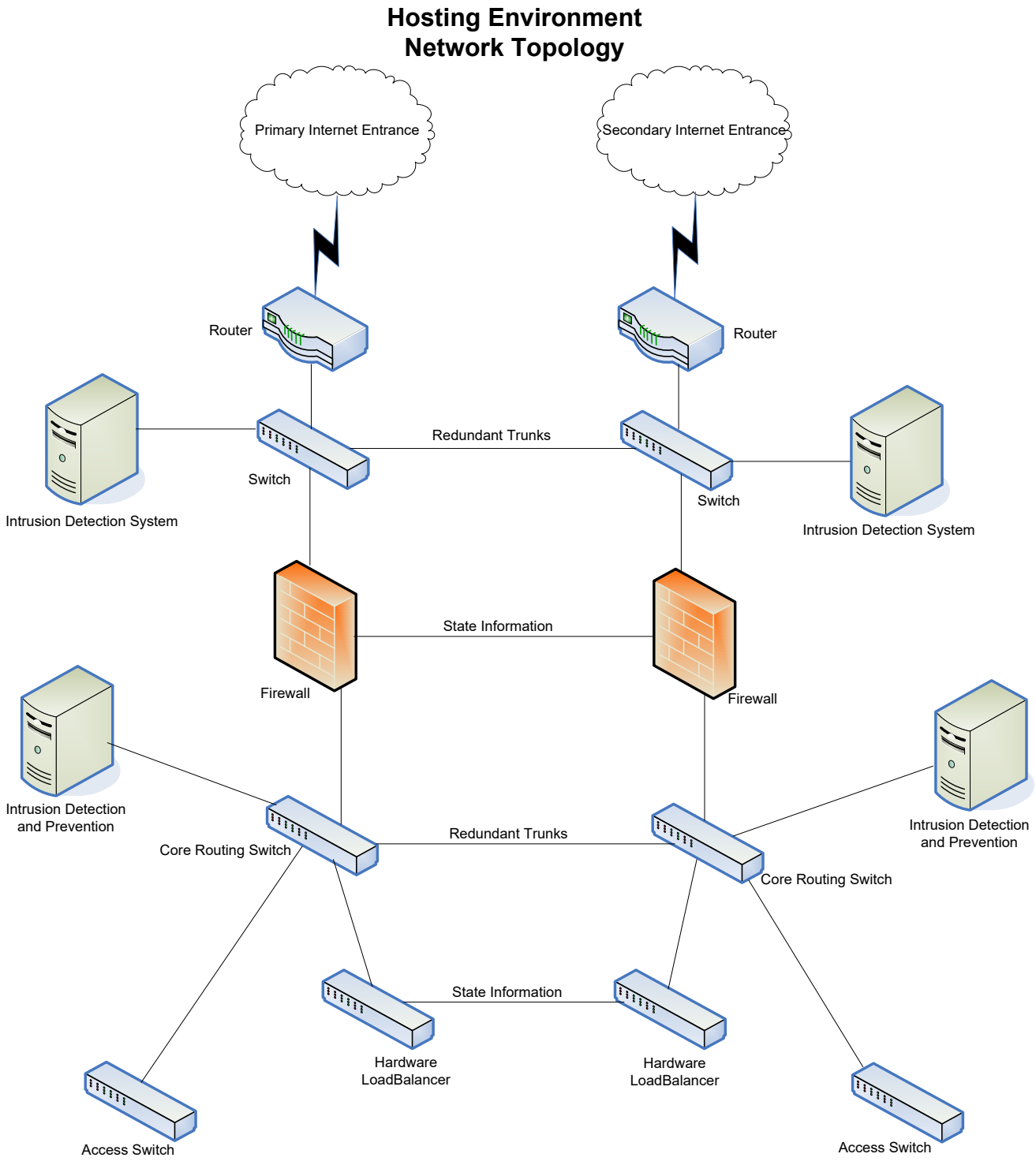
Skillsoft uses Fastly services to stream videos on Percipio.

https://www.fastly.com

Iron Mountain Offsite Storage

Skillsoft uses iron Mountain for its offiste backups storage. Iron Mountain is responsible for the secure transport and storage of the backup media. The Iron Mountain facility is located in Frankfurt, Germany.

Appendix B – PercipioTopology


Hosting Environment
Network Topology
Primary Internet Entrance
Secondary Internet Entrance
Router
Router
Intrusion Detection System
Switch
Redundant Trunks
Switch
Intrusion Detection System
Firewall
State Information
Firewall
Intrusion Detection
and Prevention
Core Routing Switch
Redundant Trunks
Core Routing Switch
Intrusion Detection
and Prevention
State Information
Hardware
LoadBalancer
Hardware
LoadBalancer
Access Switch
Access Switch