Percipio Product Document (NA & EU)

Contents

Definition Skillsoft Services (“Skillsoft”, “we”, “our”)

Introduction

This document has been created to provide a comprehensive yet high-level overview of the application, infrastructure, and security measures that we have in place to protect your data and ensure the availability and integrity of our IT systems.

At Skillsoft Services, we understand that security and reliability is of paramount importance in today's digital landscape, and we are committed to providing a secure and reliable environment for your business operations. Our IT service and system security information document covers a wide range of topics, including our security policies and procedures, physical security measures, network security, data protection, and incident management.

We have invested heavily in our security infrastructure and have implemented advanced security technologies and best practices to ensure that your data is always protected. Our security measures are regularly reviewed and updated to stay ahead of emerging threats and provide the highest level of protection.

We believe that transparency and open communication are essential in building a trusted relationship with our clients, and this document is a reflection of our commitment to transparency and accountability. We hope this document will help you understand the measures we have in place to protect your data and give you confidence in our ability to provide secure and reliable IT services.

Percipio Hosting Environment

The Percipio platform is hosted in a secure and scalable cloud environment. Skillsoft Inc utilizes Amazon Web Services (AWS) as its primary cloud provider for Percipio. AWS offers a world class infrastructure that ensures high availability, scalability, and performance of the platform.

The hosting environment is designed to meet the highest security standards and compliance requirements. Skillsoft Inc implements various security measures, such as data encryption, access controls, intrusion detection and prevention, and regular security audits and assessments, to protect user data and ensure the platform's integrity.

The platform is also designed for optimal performance and scalability. Percipio uses advanced caching and content delivery technologies to ensure fast and reliable access to learning materials from anywhere in the world. The platform can handle many concurrent users and can scale up or down dynamically based on usage patterns.

Percipio is deployed in Amazon Web Services (AWS).

North America

- Primary Operating Region is US-EAST-1
- Disaster Recovery Region is US-WEST-2

European Union

- Primary European Operation Region is EU-CENTRAL-1
- European Disaster Recovery Region is EU-WEST-1

Percipio’s hosting environment consists of multiple Availability Zones (AZ) within each region.

Percipio Application Description

Percipio is an intelligent learning platform developed by Skillsoft Inc. It provides an immersive learning experience to individuals and organizations by offering a vast collection of courses, videos, books, audiobooks, and other types of learning materials.

The platform's content library covers a wide range of topics, including leadership and management, IT and digital skills, business and finance, compliance, and safety, and many more. Users can access the content from anywhere, at any time, and on any device. Percipio also provides insightful analytics and reporting features that enable managers and administrators to track user engagement, learning progress, and overall ROI (return on investment).

Overall, Percipio is a comprehensive and scalable learning solution that helps organizations to upskill and reskill their workforce, boost employee engagement and productivity, and drive business growth.

Enhanced Learning Synchronized Assistant (ELSA)

ELSA is an optional add-on to Percipio that can be installed by the end user either as a browser plugin or as a desktop application in Microsoft Windows. ELSA is optional. Percipio will have the same functionality with or without ELSA. ELSA provides quick access to Percipio search and content from any web page via the plugin or desktop app.

ELSA does not store or process user Personal Identifiable Information (PII). Once installed ELSA will prompt the users for their organization name i.e., companyname.Percipio.com. Once the organization is validated successfully the users will be prompted for the same user ID and password used to login into Percipio. The user is validated by Percipio via the plugin. The plugin will obtain a user unique token (JWT), which is stored in the plugin. The token will off er user's seamless login for 90 days. After 90 days the token expires. The user must re-enter their credentials.

All versions of ELSA will check upon launch to see if a new version is available. The Chrome version will auto-update if a new version is available in Google store. The IE and desktop application will prompt the user to download and install the latest version.

Percipio PII and Other User Data

The table below represents the requirements and potential data types Percipio will hold as a part of service delivery.

Data Type	**Description**	**Optional?**
First & Last name	PII	Yes
Email Address	PII	No
Learning Content	Channels, Courses, books, audiobooks, videos instruction, Labs	Variable
Time spent	On Channels or Course Content	No
Collection Level Consumption	Non PII	No
Assignment Status	Non PII	No
Client Generated Content	Courseware, Additional Field as produced by Client.	Yes

High Level Architecture Considerations

Percipio service design and architecture was developed using the AWS Well Architected Framework described at the following URL.

https://aws.amazon.com/architecture/well-architected/?wa-lens-whitepapers.sort-by=item.additionalFields.sortDate&wa-lens-whitepapers.sort-order=desc&wa-guidance-whitepapers.sort-by=item.additionalFields.sortDate&wa-guidance-whitepapers.sort-order=desc

Percipio is designed to be a fault tolerant, rapidly scalable solution that provides predicably reliable delivery of training services.

- Load balancing at the network, internetwork, content delivery network, DNS (Domain Name System), and the application layer provides a resilient, redundant, and reliable service.
- Server hosts use hardened Center for Internet Security (CIS) approved images to ensure reliability and security of the server hosting environments.
- Full data path encryption ensures all information that is sent from the learner to Percipio, and back to the learner is encrypted with Transport Layer Security 1.2 and above, and all known weak cryptographic ciphers are removed from service.
- Data encryption is used for all information stored (including backups) in the Percipio environment and leverages the Advanced Encryption Standard in Galois Counter Mode with 256bit keys (AES-256 GCM).
- Use of Route53 enhances reliability and fault tolerance of the Percipio solution.
- Code and Infrastructure production, promotion and release are governed with a rigid Infrastructure as Code system development practice.

Security of the Cloud; Security in the Cloud

Operating a Cloud based service requires close collaboration between the hosting provider and their tenant. Skillsoft Percipio takes accountability for security in the cloud while AWS provides security of the cloud.

As a hosting provider and partner in security additional information regarding AWS security can be found at the following URLs.

Shared Responsibility Model
https://aws.amazon.com/compliance/shared-responsibility-model/?ref=wellarchitected

Introduction to AWS Security
https://d1.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf?did=wp_card&trk=wp_card

AWS Certification and Compliance
https://aws.amazon.com/compliance/programs/

Compliance Requirements

Federal Risk and Authorization Management Program (FedRAMP)

Percipio provides security in the cloud by maintaining an independently audited (annually) and validated security program. This program is based on meeting the control objectives of the FedRAMP control framework, which is based on the National Institutes of Standards & Technology (NIST) Special Publication 800-53 (SP800-53).

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The program was created to ensure that federal agencies have access to secure and reliable cloud computing services.

FedRAMP consists of a set of security controls and processes to which Percipio must adhere, to remain authorized to provide services to the United States Federal Government. The program is designed to assess the security of cloud services, such as Percipio.

A third-party assessment organization (3PAO) is selected to perform an independent assessment of the Percipio's security controls. We are audited for security program capability and maturity, vulnerability assessments and penetration testing of our applications and infrastructure.

Also, Skillsoft Services regularly assesses our security program capability and maturity, conducts vulnerability assessments, and penetration testing of our applications and application related infrastructure.

Finally, Percipio is subject to continuous monitoring and reporting requirements to ensure that it continues to meet the FedRAMP security requirements.

Although FedRAMP is a U.S. based Regulation, Skillsoft Services apply this rigor to all Percipio operating environments, irrespective of country or region.

FedRAMP Authorization to Operate Link

https://marketplace.fedramp.gov/#!/product/percipio?sort=productName

General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a comprehensive data protection law that came into effect on May 25, 2018, in the European Union. The regulation aims to strengthen data protection for individuals within the EU and applies to businesses that collect, process, or store personal data of individuals in the EU, regardless of the location of the business.

The GDPR establishes several rights for individuals, including the right to access, correct, or delete their personal data, and requires businesses to obtain valid consent for data processing activities, implement appropriate security measures to protect personal data, and report data breaches to the relevant supervisory authority within 72 hours.

Failure to comply with the GDPR can result in significant fines and reputational harm for businesses. Overall, the GDPR aims to ensure that businesses handle personal data responsibly, with transparency and respect for individuals' rights.

Skillsoft Services is committed to complying with the privacy objectives of the GDPR, we recognize the importance of protecting personal data and respect individuals' rights to privacy. We have implemented policies and procedures for data collection, processing, and retention, and appropriate technical and organizational measures to safeguard personal data.

We strive to provide transparency and clear communication with individuals about our data practices, obtain valid consent for data processing activities, and monitor and audit data processing activities to ensure compliance with applicable laws and regulations.

In the event of a privacy incident, we are committed to responding appropriately and promptly to mitigate any harm to individuals and address the incident's root cause.

Our commitment to complying with the privacy objectives of GDPR reflects our dedication to managing and protecting personal data responsibly, ethically, and in compliance with the highest standards of data protection.

Finally, information regarding the Citizens of the European Union is kept within the European Union.

Below is a breakout of the control families. For further details please contact your Skillsoft Sales representative, or your Account Manager.

High Level Assurance Controls

Policy, Procedure, & Process

Security policies, procedures, and processes are critical components of an effective information security program. These documents provide a clear and comprehensive framework for managing and mitigating security risks and ensuring the confidentiality, integrity, and availability of sensitive information.

Keeping these documents is crucial in today's rapidly evolving threat landscape. As new security threats emerge, it is essential to review and update these documents to ensure that they remain relevant and effective in addressing current and future security risks.

By having well-defined expectations organizations can reduce the likelihood of security incidents and minimize the impact of any incidents that do occur. These documents set clear expectations for employees and other stakeholders, helping to ensure that everyone understands their roles and responsibilities in maintaining a secure and compliant environment.

Access Control

Our company implements access control measures to protect our critical systems and data, enabling us to restrict access only to authorized personnel and minimize the risk of unauthorized access and data breaches.

Control Functions or Areas:

- Access control policy and procedures
- Account management
- Access enforcement

- Information flow enforcement
- Separation of duties
- Least privilege
- Unsuccessful logon attempts
- System use notification
- Concurrent session control
- Session lock
- Session termination
- Permitted actions without identification or authentication
- Remote access
- Access control for mobile devices
- Use of external information systems

Awareness and Training

We conduct regular training and awareness programs to educate our employees on the latest security threats and best practices, empowering them to make informed decisions and minimize the risk of human error, thereby improving our overall security posture.

Control Functions or Areas:

- Security awareness and training policy and procedures
- Security awareness training
- Security awareness insider threat training
- Role-based security training
- Security training records

Percipio Team Certification

The Skillsoft management team supports Percipio staff continuous learning which is demonstrated by our staff's held certifications. Below is a summary list of certifications:

- AWS Certified Cloud Practitioner
- AWS Certified Developer - Associate
- AWS Certified Dev-Ops Engineer - Professional
- AWS Certified Security Specialty
- AWS Certified Solutions Architect - Associate
- AWS Certified Solutions Architect - Professional
- AWS Certified Sys-Ops Administrator - Associate
- Certification in Risk and Information Systems Control
- Certified Cloud Security Professional
- Certified Ethical Hacker
- Certified Information System Security Professional
- Certified Kubernetes Administrator
- Commvault Certified Master
- FinOps Certified Practitioner

- Information System Security Architecture Professional
- Information System Security Engineering Professional
- Information System Security Management Professional
- COMPTIA Pentest+

Audit and Accountability

Our company implements audit and accountability measures to keep track of all activities on our systems and data, enabling us to identify any anomalies and hold authorized users accountable for any security breaches or violations, thereby bolstering our security measures.

Control Functions or Areas:

- Audit and accountability policy and procedures
- Audit events
- Content of audit records
- Audit storage capacity
- Response to audit processing failures
- Audit review, analysis, and reporting
- Audit reduction and report generation
- Time stamps
- Protection of audit information
- Audit record retention
- Audit generation

Security Assessment and Authorization

We ensure that our systems and data are secure our operations are compliant with relevant regulations and standards through regular security assessments, rigorous code, and infrastructure development processes and by obtaining proper authorization, mitigating the risk of security incidents and potential legal and financial penalties.

Control Functions or Areas:

- Security assessment and authorization policy and procedures
- Security assessments
- System interconnections
- Plan of action and milestones
- Security authorization
- Continuous monitoring
- Penetration testing
- Internal system connections

Configuration Management

Our company maintains the security and stability of our systems and data through proper configuration management, ensuring that all systems are adequately configured and managed to minimize the risk of security breaches and prevent any disruption to our operations.

Control Functions or Areas:

- Configuration management policy and procedures
- Baseline configuration
- Configuration change control
- Security impact analysis
- Access restrictions for change
- Configuration settings
- Least functionality
- Information system component inventory
- Configuration management plan
- Software usage restrictions
- User-installed software

Contingency Planning

We prepare for potential security incidents and other disruptions through contingency planning, developing a solid plan and response strategy to ensure business continuity even in the face of unexpected events.

Control Functions or Areas:

- Contingency planning policy and procedures
- Contingency plan
- Contingency training
- Contingency plan testing
- Alternate storage site
- Alternate processing site
- Telecommunications services
- Information system backup
- Information system recovery and reconstitution

Identification and Authentication

We prevent unauthorized access to our systems and data by implementing strict identification and authentication measures, verifying the identities of our employees and users, and ensuring that only authorized individuals can access our critical assets.

Control Functions or Areas:

- Identification and authentication policy and procedures
- Identification and authentication (organizational users)
- Device identification and authentication
- Identifier management
- Authenticator management
- Authenticator feedback
- Cryptographic module authentication
- Identification and authentication (non- organizational users)

Incident Response

Our company has a quick and efficient incident response plan in place to minimize the impact of security incidents, quickly detecting, containing, and mitigating potential breaches to protect data and systems and reduce any potential damage.

Control Functions or Areas:

- Incident response policy and procedures
- Incident response training
- Incident response testing
- Incident handling
- Incident monitoring
- Incident reporting
- Incident response assistance
- Incident response plan
- Information spillage response

Maintenance

Proper maintenance and updates are necessary to keep systems and data secure. By conducting regular maintenance to ensure that our systems remain up to date, it reduces the risk of security incidents and minimizes downtime.

Control Functions or Areas:

- System maintenance policy and procedures
- Controlled maintenance
- Maintenance tools
- Nonlocal maintenance
- Maintenance personnel
- Timely maintenance

Media Protection

We take measures to protect our physical and digital media, which can contain sensitive data, by implementing proper media protection measures to minimize the risk of data loss or theft.

Control Functions or Areas:

- Media protection policy and procedures
- Media access
- Media marking
- Media storage
- Media transport
- Media sanitization
- Media use

Physical and Environment Protection

We protect our physical facilities and equipment from security threats by implementing physical and environmental protection measures to minimize the risk of theft, damage, or other security incidents.

Control Functions or Areas:

- Physical and environmental protection policy and procedures
- Physical access authorizations
- Physical access control
- Access control for transmission medium
- Access control for output devices
- Monitoring physical access
- Visitor access records
- Power equipment and cabling
- Emergency shutoff
- Emergency power
- Emergency lighting
- Fire protection
- Temperature and humidity controls
- Water damage protection
- Delivery and removal
- Alternate work site

Additionally, AWS has a very stringent regime for controlling access to their data center facilities ("the cloud"). The URL provided below provides insight into those controls.

AWS Data Center & Facility Controls
https://aws.amazon.com/compliance/data-center/controls/

Planning

We develop effective security strategies by conducting thorough planning and risk assessments, identifying potential threats, and developing mitigation strategies that align with our business objectives.

Control Functions or Areas:

- Security planning policy and procedures
- System security plan
- Rules of behavior
- Information security architecture

Personnel Security

Our employees are our first line of defense against security threats, and we ensure their trustworthiness and provide proper training by implementing personnel security measures to minimize the risk of insider threats and human error.

Control Functions or Areas:

- Personnel security policy and procedures
- Position risk designation
- Personnel screening
- Personnel termination
- Personnel transfer
- Access agreements
- Third-party personnel security
- Personnel sanctions

Risk Assessment

We identify and prioritize potential security risks by conducting regular risk assessments, focusing our resources on the most critical areas, and minimizing the risk of security incidents.

Control Functions or Areas:

- Risk assessment policy and procedures
- Security categorization
- Risk assessment
- Vulnerability scanning

System and Services Acquisition

We ensure that any systems or services we acquire meet our security requirements and standards by implementing proper system and services acquisition measures, minimizing the risk of vulnerabilities and other security issues.

Control Functions or Areas:

- System and services acquisition policy and procedures
- Allocation of resources
- System development life cycle
- Acquisition process
- Information system documentation
- Security engineering principles
- External information system services
- Developer configuration management
- Developer security testing and evaluation

System and Communications Protection

We protect our systems and data from unauthorized access and other security threats by implementing rigorous system and communications protection measures, safeguarding our critical assets, and minimizing the risk of security breaches.

Control Functions or Areas:

- System and communications protection policy and procedures
- Application partitioning
- Information in shared resources
- Denial of service protection
- Resource availability
- Boundary protection
- Transmission confidentiality and integrity
- Network disconnect
- Cryptographic key establishment and management
- Cryptographic protection
- Collaborative computing devices
- Public key infrastructure certificates
- Mobile code
- Voice over internet protocol
- Secure name /address resolution service (authoritative source)
- Secure name /address resolution service (recursive or caching resolver)
- Architecture and provisioning for name/address resolution service
- Session authenticity
- Protection of information at rest
- Protection of information at rest | cryptographic protection
- Process isolation

System and Information Integrity

We ensure the trustworthiness and reliability of our data and systems by implementing measures to maintain system and information integrity, such as data validation, data encryption, and system monitoring, to prevent unauthorized modifications, ensure data confidentiality, and minimize the risk of data loss or corruption.

Control Functions or Areas:

- System and information integrity policy and procedures
- Flaw remediation
- Malicious code protection
- Information system monitoring
- Security alerts, advisories, and directives
- Security function verification
- Software, firmware, and information integrity
- Spam protection

- Information input validation
- Error handling
- Information handling and retention
- Memory protection

Final Statement

We hope that this high-level Information Technology (IT) service and system security information document has provided you with valuable insights into the security measures that we have in place to protect your data and ensure the availability and integrity of our IT systems.

Skillsoft Services, we are committed to providing the highest level of security for your business operations, and we believe that transparency and open communication are key to building a trusted relationship with our clients.

We encourage you to review this document carefully and reach out to us if you have any questions or concerns. We are always here to help and are committed to working with you to ensure that your data remains secure and always protected.