Learning Management System (LMS) Security Statement
Contents

Introduction ................................................................................................................................................. 3
Networking Architecture ........................................................................................................................... 4
Firewalls and Intrusion Prevention System .................................................................................................. 7
  File Upload Protections .......................................................................................................................... 7
  SQL Injections ........................................................................................................................................ 7
  XSS - Cross-Site Scripting ....................................................................................................................... 7
  CSRF - Cross-Site Request Forgery ......................................................................................................... 8
  Antivirus .................................................................................................................................................. 8
Updates and Upgrades .................................................................................................................................. 9
  Regular Maintenance Updates ................................................................................................................ 9
  Upgrades .................................................................................................................................................. 9
  Upgrades and Updates Policy ................................................................................................................ 9
Compliance and Certifications ..................................................................................................................... 11
Monitoring and Auditing ............................................................................................................................. 12
Disaster Recovery and Business Continuity .................................................................................................. 13
User Related Security Policies .................................................................................................................... 14
Password Restriction Policies ...................................................................................................................... 15
Data Center Facilities ................................................................................................................................... 16
Data Stored by Docebo ............................................................................................................................... 18
Application Level Security .......................................................................................................................... 19
  Cookies .................................................................................................................................................... 19
  Sessions .................................................................................................................................................... 19
  Content Protection .................................................................................................................................... 20
  Content Encryption ................................................................................................................................... 20
Vulnerability Scanning ................................................................................................................................. 21
Hosting Access ............................................................................................................................................ 21
Hosting Location .......................................................................................................................................... 21
Support ....................................................................................................................................................... 21
Introduction

Compliance Learning is built on a state-of-the-art world class Learning Management System (LMS) provided by Docebo. The application is hosted on secure cloud on Amazon Web Services (AWS).

The following document provides an overview of the architecture and the implementation of several layers of industry security standards to ensure safety, data privacy and confidentiality of our clients.
NETWORKING ARCHITECTURE

The LMS adopts an architecture which involves the duplication of the system’s critical components or functions in order to increase their reliability. The functional chart below describes this architecture in greater detail.

Following is the more detailed descriptions of the components involved:

Amazon route53 geo-DNS
A DNS is an Internet service that resolves web addresses (www.example.com) into a numeric IP address (127.12.0.2). The Route 53 DNS by Amazon guarantees high standards of scalability and availability to ensure the best possible performance. The DNS service is also configured to leverage the latency DNS resolution that allows Docebo to serve users’ requests from the nearest available datacenter.

Amazon ELB
An Amazon ELB is a network component that allows us to redistribute the traffic load between multiple servers.
VPC
The Amazon Virtual Private Cloud (VPC) allows Docebo to maintain a logical isolation between the Docebo architecture and the Amazon resources, regulating access to the different architecture components.

LMS-Routing Layer
This is the only layer exposed to the Internet. It performs the following tasks:

1. Intelligent routing between the different back-end services. The correct service is selected based on the client domain and the corresponding architecture load for load balancing purposes.
2. Serving static non-private resources via cache to the end-user
3. Intrusion Detection System
4. Intrusion Prevention System
5. SNI resolution support

NOSQL layer for routing configuration caching
These are servers that store the information needed for routing. The same servers are also used for caching purposes.

LMS-APP
The Apache/PHP web servers implement the application’s logic in resolving users’ requests.

Separate Datacenters
Separate datacenters are used in the duplication of the system’s critical components or functions. This increases the reliability of these services. They are also involved in any disaster recovery process.

LMS-DB-Master
The master MySQL database servers are kept on the first availability zone.

LMS-DB-Replica
The mirrors of the master MySQL database that are kept up-to-date in real time by the master database.

Vpn-gw-management
The Docebo technical team uses this Vpn server to access the infrastructure for support and maintenance purposes. Only Docebo-authorized personnel have access to the server – and only then via a unique, individualized identifier.

Docebo Content Delivery Layer (DCD)
All content delivered by the Docebo LMS comes via the DCD servers. These servers implement a secured digital signature system that generates a unique link every time a resource is accessed by an end-user. This also generates a unique URL.
Amazon S3
All the user-generated content is stored inside the secured Amazon S3 object storage and delivered via the Docebo Content Delivery layer. Enterprise customers can request their own dedicated S3 storage bucket as an additional service.

Databases
Docebo adopts MySQL technology for Database management purposes. Files uploaded by users or automatically generated by the application (e.g. certificates) are not stored into the database but on an object storage (Amazon S3). Below is the complete list of files stored in S3:

- SCORM and Tin Can assets
- Videos
- Downloadable assets
- Learners’ assignments
- Students’ answers to test assessments
- SlideConverter related assets
- Course widget downloadable files
- Course logos
- Course backgrounds
- Logos
- Favicon
- Login page image
- Users’ avatars
- PDF certificates
- Images uploaded using the WYSIWYG text editor

Each database is created at the time of activation of a new Docebo LMS instance, and a dedicated database user is created during the process. From a database management standpoint, Docebo maintains rigorous policies about keeping each customer’s data and information secured and separated from one instance to the other. This is valid for both the Docebo LMS product as well as the Docebo Enterprise Cloud product. It is by leveraging the capabilities of the Cloud infrastructure, in combination with the MySQL technology, that Docebo keeps each customer’s information inside dedicated databases with separate access for respective data sets.
FIREWALLS & INTRUSION PREVENTION SYSTEM

At the routing level, Docebo has implemented both an intrusion detection system and an Intrusion prevention system. These systems monitor and analyze the traffic and identify any possible malicious connection or request. They also automatically block the traffic source and notify Docebo staff in case of any suspect event.

Connections to the Docebo architecture are checked with real-time log analysis and correlation engines. These monitor the connection attempts and the successful connections through the log (SSH, http and so on). They match them with a predefined set of rules to identify possible break-in attempts or malicious connections.

FILE UPLOAD PROTECTIONS

New files uploaded in the Docebo LMS are checked against a whitelist of allowable file types. They are discarded if they do not match, prior to making the resources available to the end users. If the first check is passed (whitelist check), when the file is completely uploaded but before it is stored in its final position, it is inspected using Enterprise Antivirus software to identify malware or viruses. If this check identifies a possible threat, the uploaded file is immediately discarded. The virus definition database is continuously and automatically updated to match the latest information on viruses.

If both verification steps are passed successfully, the file is then copied to the final storage unit. This is not directly accessible from the web-servers and does not have any self-executable permission.

SQL INJECTIONS

An SQL Injection is a hacking technique that targets applications that use SQL databases. It tries to inject malicious code into SQL queries in order to retrieve extra information or to change some of the application’s behavior.

In order to prevent SQL injection, the application protection checks the input data sent from the client to the server and removes any harmful codes before it is used in a query on the database.

This precaution is used to prevent the insertion of malicious data, the overwriting or deletion of data, or information leaking.

This protection checks the input data sent from the client to the server and removes any harmful codes before it is used in a query on the database. This precaution is used to prevent the insertion of malicious data, the overwriting or deletion of data, or information leaking.

XSS – CROSS-SITE SCRIPTING

XSS Scripting is a hacking technique that targets web applications. It attempts to show malicious scripting (in other words javascript) code to an end user in order to collect data from that user or to redirect the user to other sites.

In order to prevent XSS type malicious activity, Docebo implements an input filter. This filter cleans up the information sent to the LMS before it is saved in the database. This filtering ensures that the end user is always presented with cleansed information.

The filter that cleans up the users’ input operates with a whitelist approach. It removes what is not allowed by the whitelist and also ensures that the html input is valid and well formatted.
CSRF – CROSS-SITE REQUEST FORGERY

CSRF attacks use URLs generated from outside our application with the aim of getting them to perform unwanted operations. To prevent CSRF attacks, Docebo implements a random token that is associated with the session itself. Every AJAX action or edit action should, therefore, carry a valid token. The application will only accept the request if the token that is sent with the request matches the one associated with the valid user session. In this way, if the request is generated from outside the application, the tokens will not match and the request will be refused.

ANTIVIRUS

**see file upload protection**
UPDATES AND UPGRADES

The following definitions of updates and upgrades apply:

REGULAR MAINTENANCE UPGRADES

This consists of minor releases that relate to either bug fixes or minor service improvements which, during deployment, do not affect the LMS’s stability, performance and/or standard behavior, and which can be applied without service interruption. These also do not require a notice time as they are considered part of the standard service housekeeping executed by Docebo on both the standard and Enterprise clusters.

UPGRADES

This refers to the implementation of a new “build” or “version” of the software that includes brand new functionalities in the system, or to a refactoring (i.e. improvement) of pre-existing functionalities. These upgrades can be subdivided into two subcategories, namely Major Upgrades and Minor Upgrades.

Major Upgrades

These are also commonly referred to as new Major releases, and can contain major service/structural refactoring that may, or may not, affect the end user’s experience and/or the user interface. Alternatively, they may change the way some features are implemented. The purpose of these upgrades is to add brand new capabilities that extend the product usability. Examples of a Major upgrade may include a User Interface revamp along with additional functional modules. The average release cycle of Major upgrades is 18 to 24 months.

Minor Upgrades

These can be used to add a new feature as well as additional feature components. They cannot consist of a radical product UI change. The main objective of Minor upgrades is to provide product differentiation without creating an entirely new or different product in terms of the UI. Examples of a minor version may be the release of new Docebo APPs to extend the system’s ability to achieve a specific missing behavior or task. The average release cycle of Minor upgrades is between three to four months.

UPGRADES AND UPGRADES POLICY

The policies for the service updates and upgrades depend upon the type of service to which the customer is subscribed. Please see below the policies in place for both of the Docebo services: LMS and Enterprise.

Docebo LMS Related Policies

Updates and upgrades are scheduled at Docebo’s discretion and are scheduled by giving notice to customers via the appropriate product newsletter. In the case of Major Releases only, Docebo SaaS customers are able to test the new release prior to transitioning to the newly released version, for an average period of three months. After this, all customers will be massively migrated to the latest service version.
Docebo Enterprise Cloud Solution Related Policies

Minor upgrades are released automatically, with prior notification to the customer. Major upgrades are released on client request and based on a mutually agreed timeframe. The process for major upgrades often involves the release of a temporary QA platform (sandbox) in which the customer can test the new Major Version prior to proceeding to full system migration. A client is allowed to stay on a specific major version for an average of one major version cycle. For instance, if Docebo releases a new version 7.x, customers currently on the version 6.x will be requested to migrate once the version 7.x is made available, and will be forced to migrate prior to the planned release of the following major version 8.x. It is important to note that if you remain on an old major version for more than 12 months after a new major version has been released, we cannot guarantee the SLA on the opened tickets.

Any updates to software that is integrated into Docebo by Thomson Reuters will undergo extensive review and testing to ensure our products meet the highest quality standards. Updates relating to security will go through additional reviews by our security specialists our deployment plan is based on our current patch policy. Where appropriate, additional controls may be implemented to mitigate against identified threats.
COMPLIANCE AND CERTIFICATIONS

As Docebo understands that security and reliability are critical elements in the choice of a Cloud-based software solution, it maintains high security standards and, in line with such standards, carefully selects its providers by partnering with those organizations that not only prove the highest industry ratings in their specific services but also ensure the highest level of reliability and security.

Docebo is certified in:


Amazon Web Services (AWS), the world’s leader in Cloud and CDN provisioning for software vendors, has garnered an extensive number of certifications. The following link provides extensive information and data related to risk management and risk prevention associated due diligence:


Seeweb, our additional and European based ISP provider, is certified as well, according to the following documentation made available below:

MONITORING AND AUDITING

Docebo’s architecture is built in a redundant (reliable) manner, to properly mitigate and reduce any possible drawbacks caused by outages to specific architectural components, and avoiding taking on a single point of failure.

In order to monitor its production and staging architecture, Docebo adopts a separate and independent architecture. By leveraging the use of state-of-the-art and leading monitoring tools, Docebo collects all data related to the different systems in a virtual control dashboard. This allows the identification of any warning, outage or performance reduction in the infrastructure.

The same data is checked via an external monitoring system and, if any anomaly is found or the data seems inaccessible, an incident notification is immediately sent to the relevant parties. The external monitoring is performed via an advanced ICMP, SNMP traps and HTTP monitoring tool. This is a reliable third-party SaaS monitoring system that can check multiple systems and send multi-channel notifications concurrently via email/SMS to the dedicated 24/7 on-call support personnel.

The monitoring system performs system checks every 60 seconds. In the event that, after a number of checks (five) a non-automatically recoverable error is identified, an incident is filed and the Docebo technical staff are notified via email and the managers via SMS notification.

Uptime and downtime tracking records are traced via the Docebo monitoring service and are reported on the Docebo website. In particular, the uptime percentage and availability is calculated over a period of 30 days.

Communication related to outages is kept on an official page on the Docebo website: HTTP://DOCEBO.STATUS.IO/
DISASTER RECOVERY AND BUSINESS CONTINUITY

The Docebo infrastructure scores highly when it comes to levels of availability and to providing customers with the features to deploy a resilient IT architecture.

The Amazon Data Center Business Continuity Management is under the direction of the Amazon Infrastructure Group. Available data centers are built in clusters in various global regions. All data centers are online and serving customers. No data center is “cold”. In case of failure, automated processes move customer data traffic away from the affected area. Each availability zone is designed as an independent failure zone.

Docebo leverage this capability by balancing the architecture components between two Availability Zones to keep the system operational, even if one Availability Zone stops working. In case of an Availability Zone failure, the DNS is configured to exclude the unhealthy services from the pool of available services and redirect the traffic to the operational Availability Zone. To cover the increase of traffic in the new zone, the automatic scalability process will begin creating the extra resources needed to keep the service at an acceptable response level.

When the original Availability Zone is back online, the Docebo team follow a standard procedure to remove the old services that are out of sync from the Availability Zone (databases, routes, and so on). They will then recreate the needed system and link this with the other Availability Zone.

When all the systems are reconfigured, the services in the Availability Zone are relinked in the DNS and the traffic will start flowing again into the original data center.

Communication related to outages is kept on an official page on the Docebo website: HTTP://DOCEBO.STATUS.IO/

For more information related specifically to the Amazon Datacenter, you can refer to this document: http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
USER RELATED SECURITY POLICIES

In Compliance Learning, each user is required to verify their login using unique credentials (username and password) in order to access the system, regardless of the user’s role in the system. Anonymous logins are not permitted. The Learning Management System (LMS) allows administrators to configure different levels of complexity in password management, depending on their housekeeping and internal security policies.

However, in most cases, Docebo can also provide alternative authentication methods via diverse Single Sign On (SSO) modalities. These ways of delivering simple access to the system are usually either built-in products or bespoke integrations with one of the following applications or authentication systems:

The most popular legacy systems used by clients’ IT departments involve:

- HR systems (Workday, Cezanne, PeopleSoft, SAP)
- ERPs (Oracle)
- CRMs (Sugar, SF.com)
- Other legacy tools

The most popular Docebo built-in authentication APPs:

- LinkedIn
- Google Apps
- Gmail
- Facebook
- Twitter

The most popular Docebo built-in authentication methods:

- ADFS (Secured Federated Active Directory)
- LDAP
- SAML
- Ad-hoc secured authentication via token based signed URL
PASSWORD RESTRICTION POLICIES

The Learning Management System (LMS) allows administrators to configure different levels of complexity in password management, depending on their housekeeping and internal security policies. Some of the password-related capabilities from an LMS administrator’s standpoint are to:

- Set a minimum password length 4
- Request to create a password with mixed alphanumeric characters
- Set an automatic expiration for passwords
- Request a change of password at user next sign-in
- Forbid the usage of previously used passwords

Please note that all the passwords are stored in the Docebo database within a highly secured (encrypted hash), non-reversible algorithm. Therefore, the Docebo staff are unable to retrieve a previously stored password by any user in the system/database. However, users can use the password recovery functionality to be guided into setting up a new password.
DATA CENTER FACILITIES

Docebo has assessed and selected two leading vendors for its Cloud-related services. The following providers are fully integrated in the Docebo technology pack:

- Amazon Web Services
- Seeweb

The datacenter for both providers is built and maintained with state-of-the-art procedures and technologies. The following information applies to both providers.

Access to the Premises
Access to the datacenter is strictly limited to the ISP employees and suitably authorized third-party personnel. Neither the general public nor clients are granted access to this infrastructure.
Access to the datacenter requires access to the ISP’s office via physical key and badge recognition with a secret code. In addition, access to the datacenter is further subject to authorization via a smart card. These cards are only possessed by personnel authorized to work in the datacenter.
All access to the premises is logged by a computer. Any third party entries take place exclusively in the presence of in-house personnel. These entries are recorded by checking the reason and access authorization. Any authorization granted is only valid for the access period.

Surveillance of the Premises
The premises are monitored 365/366 days a year, 24 hours a day, by security personnel and/or by video-surveillance systems. External perimeter video-surveillance is provided by TV cameras and recorded according to image retention rules adhering to the law.

Intrusion Detection
An intrusion-detection system monitors access to hallways and provides continuous monitoring of all rooms in the office and datacenter, with local optical/acoustic signals and remote notification.

Fire Detection and Suppression
Automatic fire and smoke detection and suppression equipment have been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all datacenter spaces, mechanical and electrical infrastructure areas, chiller rooms and generator equipment rooms.
Temperature Control
The air-conditioning system provides air-filtration and internal ventilation and cooling, thus guaranteeing the correct temperature and sufficient air circulation. Its operating parameters are constantly measured. Local and remote alarms are triggered when critical values are exceeded.

Power Supply
The power supply system is designed to be fully reliable (redundant) on double EIE-CE standard lines for each row of cabinets with anti-tear fireproof plugs, and sockets to guarantee 24 hours a day, 365/366 days a year functionality.
Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure for critical and essential loads in the facility. Datacenters use generators to provide backup power for the entire facility.

For more information related specifically to the Amazon Datacenter, you can refer to this document: http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
DATA STORED BY DOCEBO

The following data is stored in the learning technology applications.

User Profile
User profiles can be imported into the application during initial implementation. User information may include First Name, Last Name, Email Address, Group Hierarchy, as well as up to three reference fields as per client needs.

Course Level Tracking
Course level data tracking includes a user’s Enrollment Status, Pass/Fail Result, Score (best), Date Enrolled, Date Completed and Deadline. For analytic purposes, certain types of courses also track Number of Attempts, Previous Scores, Time Spent and meta-data on Red Flag and Question Responses.

Assessment Level Tracking
Assessment level data tracking includes a user’s Enrollment Status, Pass/Fail Result, Score (best), Date Enrolled, Date Completed, Deadline, Number of Attempts, Previous Scores and meta-data on Question Responses for analytic purposes.
APPLICATION LEVEL SECURITY

Access to the LMS can be limited to connecting only through a secure connection. This ensures that all the data exchanged between Docebo’s servers and the client’s PCs are securely encrypted. The Docebo LMS standard products make available the use of an SSL/HTTPS connection via the Docebo wildcard certificate. The Docebo LMS wildcard certificate has the following characteristics:

- It is issued by GeoTrust, which is used as certification authority
- It has one year validity. Thereafter, the certificate is renewed and the keys rotated
- A key strength of 2048 bit
- Connection performed with 256 bit encryption

Our termination endpoint for encrypted connection is the routing layer at the entrance of the VPC. The endpoint supports the following TLS/SSL versions: TLSv1, TLSv1.1, TLSv1.2 and uses the SNI standard implemented by all our officially supported browsers.

For any customer bespoke domain (meaning those Docebo instances that do not apply the xxxx.doceboasaas.com domain policy), the use of SSL/HTTPS requires a dedicated certificate. This must be supplied by the client using the CSR (Certificate Signature Request) provided by Docebo.

COOKIES

Docebo uses browser cookies in order to send the user to the correct backend server and to keep the sessions linked. All the cookies generated by Docebo are marked for http-only. This makes them inaccessible and not editable through browsers and javascripts. No cookies contain users’ personal data, or are ever used for the purpose of advertising and/or marketing-related userprofiling. Nor does any cookie-generated data ever provide any user-related information to third parties.

SESSIONS

Users’ sessions are maintained inside a central database repository. The association between a session and the user assigned to that session is performed via a session identifier and cookie only. This solution, in conjunction with the use of a secure connection with https, prevents the possibility of session hijacking.

To prevent session replay, the identifier is automatically generated leveraging the OS random seed generator and every new identifier is checked against conflict before usage.

Sessions are checked for unique logged-in users. If two separate sessions are identified simultaneously by the same username, the first one will be forced to log out from the system.

Expired sessions are identified through a pre-configured idle time. If the user performs an action outside of the idle time, then the session is marked as expired and the user is asked to sign-in again. If needed, the idle time can be increased or decreased through the LMS settings.
At predefined times, a garbage collector scans for sessions that have been abandoned and have been inactive longer than the idle time specified. Subsequently, it destroys these sessions.

**CONTENT PROTECTION**

Docebo delivers static content through its designated Amazon related Content Delivery Network (CDN). In this situation, the delivery of the content can leverage the caching and the proximity of the CDN endpoints to the final user.

The content delivered by Docebo through the CDN uses auto-expiring URLs. Every resource (video and SCORM in general) served by the system via the CDN comes with a signed URL. This URL will automatically expire within 60 minutes and will not be re-usable to access the same information. In order to access the information again, a new signed link would have to be generated.

**CONTENT ENCRYPTION**

Content encryption over the network between Docebo servers and clients can be achieved with the use of https. Docebo also provides solutions that deliver encryption to the content at the storage level as an additional service.

Files uploaded by the users are stored inside Amazon S3. It is possible to leveraging the capability of the service to store the file with a 256-bit AES encryption.
VULNERABILITY SCANNING

Docebo works with 3rd party company (NOPSEC) that specializes in software vulnerability testing to find and remediate any vulnerabilities that their system might have. NOPSEC performs vulnerability tests on cross site scripting, path traversal, unrestricted file uploads, and SSL cookie set without secure flag. NOPSEC provides and a detailed report on its vulnerability findings, so that Docebo can work to improve any vulnerabilities that may be uncovered.

Thomson Reuters also performs vulnerability scanning on any integrated code with Docebo. Our internet-facing sites are undertaken regularly across the global network, and policy compliance software is used to ensure systems are maintained in accordance with security requirements. Specialist penetration testing companies are also engaged to provide a further level of assurance.

HOSTING ACCESS

In order to ensure successful network access to Docebo, your network team may be required to add the following URL’s to your company’s approved “whitelist” register to ensure these entities are accepted, approved and/or recognized.

- Your custom domain – (Optional feature and differs by company. Please consult with your implementation specialist.)
- Docebosaas domain - https://tr-red-live.docebosaas.com
- CDN - https://d36sp15w3z9i0o.cloudfront.net
- Angular CDN - https://dmdfxzlkevsyu.cloudfront.net
- Web socket host - https://wss-tr.docebosaas.com/

HOSTING LOCATION

Compliance Learning via Docebo is currently physically hosted by Amazon Web Services in EMEA (Dublin, IRE). All data (learners, courses, learner history) within Docebo is stored in this location.

Static content (javascript, CSS and images) are distributed, accessed and delivered via Amazon Cloud Front which is a Content Distribution Network (CDN) and is done to improve performance of Docebo across the globe.

SUPPORT

Thomson Reuters and Docebo have created an incident management process and associated support process workflows which outline the efficient management of 4 common types of incidents which may occur. Here is a brief description of the types of incidents which may occur:

**URGENT (or Priority 1)** – A Docebo Production service is completely down or unresponsive to web browsing. Certain APIs which are non-responsive and may also cause a potential impact within this severity.

**HIGH (or Priority 2)** – A Docebo Production service may have degraded performance or capacity.
NORMAL (or Priority 3) – These incidents affect normal business processes within Compliance Learning and are likely caused by incorrect or inoperable functions of Docebo.

LOW (or Priority 4) – These incidents have little or no effect on normal business processes within Compliance Learning. They may be caused by incorrect or inoperable functions of Docebo but are not required daily or are rarely used.

Thomson Reuters has established various Service Level Agreements for the services provided by Docebo. This includes:

**AVAILABILITY TARGETS** – This agreement establishes the service availability target for Docebo and is calculated and reviewed quarterly. This includes establishing expectations around Excused (Planned maintenance, Emergency downtime) and Unexcused outages and affects the calculation for availability of Docebo’s services.

**SERVICE TARGETS** – These outline service expectations for Initial Response from support for an incident, Ongoing Communication expectations while resolving an incident and the Incident Mitigation Target for each type of incident.

Thomson Reuters has also established an incident management process with Docebo to ensure efficient handling and communication of incidents which may occur. A simple view of the incident management is shown here: