360learning

UPSKILL FROM WITHIN

Technique Documentation

Version 6.5 (Août 2025)

A 360Learning, nous ne faisons aucune promesse concernant les solutions techniques, nous prenons des engagements.
Vos données vous appartiennent. Elles sont et resteront à votre disposition.
Vous, et vous seul.

APPRENTISSAGE À 360° EST UN FOURNISSEUR EUROPÉEN DE SOLUTIONS CLOUD DE PREMIER PLAN

> En tant que fournisseur leader de solutions cloud, nous nous engageons à offrir à nos clients des niveaux élevés de sécurité, de SLA et de confidentialité, tant dans nos engagements contractuels que dans l'infrastructure technique que nous développons. Nous respectons les exigences légales françaises, les plus strictes en matière de données, de sécurité et de confidentialité.

Benjamin Marchal
PDG, 360Learning

Pour plus d'informations, veuillez nous contacter:

produit@360learning.com / www.360learning.com

360learning

Table des matières

Vos données vous appartiennent

C'est vraiment le cas

Le client conserve la propriété des données hébergées sur 360Learning.

À la fin du contrat, les clients peuvent demander à 360Learning de récupérer leur catalogue de cours dans son intégralité dans un format standard.

Nos droits

Les employés de 360Learning n'ont accès aux données du client que dans certains cas spécifiques :

- Questions des clients sur leurs données
- Résolution de problèmes
- Demandes du client pour modifier les données

Confidentialité

360Learning garantit qu'aucune donnée personnelle à laquelle elle a accès en tant que sous-traitant de données pour fournir des services contractuels n'est vendue, transférée ou divulguée à des fins commerciales à des tiers.

Pseudonymisation

360Learning garantit que les données personnelles sont isolées dans un ensemble unique de nos bases de données, et que toutes les autres données métiers (contenus de formation, statistiques de formation, groupes, parcours...) utilisent un identifiant aléatoire pour référencer chaque utilisateur, garantissant une pseudonymisation des données personnelles conformément au RGPD.

Disponibilité

1. Configuration minimale

PLATE-FORME

Une configuration minimale est requise afin de profiter pleinement de l'application 360Learning :

- Vérifiez les prérequis suivants du poste de travail : résolution d'affichage minimale de 1 024 x 600 pixels et 256 Mo de RAM.

- Assurez-vous que tous les ordinateurs disposent d'un navigateur compatible : Microsoft Edge, Mozilla Firefox, Google Chrome ou Apple Safari dans une version prise en charge par le fournisseur.

- Réaliser des tests de bande passante réseau afin de déterminer la bande passante disponible pour les formateurs et les apprenants, et optimiser la configuration réseau en fonction du type de formats d'enseignement proposés, pour une diffusion et une consommation optimales du matériel pédagogique.

Débit minimum requis pour la connexion Internet : 512 kbps par poste pour toute utilisation y compris le streaming vidéo (selon les conditions précisées au paragraphe « Vidéo » ci-dessous) et hors cours SCORM.

- Authentifiez les serveurs de messagerie afin de garantir que les e-mails envoyés par la plateforme ne soient pas bloqués par le service informatique du client. L'adresse e-mail no-reply@360learning.com doit être ajoutée à la liste blanche dans le champ « De » (et non dans le champ d'adresse du serveur SMTP) des paramètres du client de messagerie, du serveur de messagerie et du logiciel antispam. Si vous personnalisez ultérieurement l'adresse e-mail pour les notifications de la plateforme, vous devrez également l'ajouter à ces emplacements. Si vous ne pouvez pas filtrer sur le champ « De », vous pouvez ajouter à la liste blanche les adresses IP suivantes :

  IP d'environnement de pré-production :
  - 20.40.143.206
  - 20.74.25.131

  IP de l'environnement de production :
  - 51.138.202.254
  - 20.74.1.94
  - 20.74.25.229
  - 52.252.128.38
  - 52.252.135.139
  - 20.88.12.20
  - 54.240.50.244
  - 54.240.50.243

- Liste blanche *.360learning.com ou le nom de domaine personnalisé pour garantir que les membres peuvent accéder à la plateforme.

- Ajoutez les domaines ci-dessous à la liste blanche pour accéder aux banques d'images Unsplash et Pixabay
  https://unsplash.com/*

https://pixabay.com/*

- Facultatif : si vous prévoyez d'utiliser des cours SCORM, assurez-vous que les fenêtres contextuelles sont autorisées.

- Facultatif : ajoutez api.amplitude.com et cdn.amplitude.com à la liste blanche afin que le département R&D de 360Learning dispose des outils d'analyse nécessaires pour détecter les erreurs, corriger les bugs le plus rapidement possible et améliorer l'expérience utilisateur en continu.

Pour vous aider à vérifier tous les prérequis techniques et tester votre plateforme avant son déploiement, utilisez les checklists disponibles dans notre guide :

- 360Learning - Guide technique - Procédure de validation

SUPPORT MOBILE

Versions prises en charge :

- iOS 16 et supérieur
- Android 7.0 et supérieur

Sur les appareils mobiles, nous prenons uniquement en charge nos applications mobiles natives. Bien que notre plateforme soit responsive design, nous ne prenons pas en charge les navigateurs web mobiles. Toute sortie d'application personnalisée ou mise à jour/mise à niveau d'application mobile est soumise aux délais du marché d'applications concerné (Google Play Store, Apple App Store…) qui restent hors de notre contrôle.

Nos applications mobiles prennent principalement en charge les cas d'utilisation de l'apprenant, mais prend également en charge certains cas d'utilisation du coach et du manager.
En outre, ils prennent en charge une large gamme d'artefacts de cours et de formats de fichiers, notamment :

- Aide-mémoire de cours et questions natives 360Learning
- Images (gif, jpg, png, bmp, ico, heic)
- Vidéos (3gp, avi, flv, m2ts, m4v, mkv, mov, mp4, mpeg, mpg, mts, vob, webm, wmv)
- Fichiers PDF
- Documents Microsoft Office (docx, xlsx, pptx)
- Contenu partageable depuis le Web (lien direct, code d'intégration ou code iframe ; nécessite une connexion Internet)

VIDÉO

360Learning prend en charge le téléchargement de vidéos HD et crée automatiquement des versions SD, en moyenne cinq fois plus petites que les fichiers originaux. Un sélecteur HD/SD est disponible en bas à droite du lecteur pour permettre aux utilisateurs de définir la qualité de streaming souhaitée. Veuillez noter que le lecteur adapte automatiquement la qualité vidéo à la bande passante disponible et que l'utilisation de la HD consomme davantage de bande passante réseau.

Afin de gérer l'utilisation de la bande passante, assurez-vous que le débit de vos fichiers vidéo est inférieur ou égal au débit attendu du réseau cible. Par exemple, si la bande passante SD et HD souhaitée doit être inférieure à 512 kbit/s, veuillez télécharger les fichiers sources avec un débit inférieur à 512 kbit/s.

2. Contenu

La plateforme 360Learning prend en charge la création de feuilles de triche et de plusieurs types de questions, telles que vrai/faux, choix multiples, réorganisation, liaison, zones sensibles, questions ouvertes, entre autres.

Vous pouvez également importer différents types de documents :

- Audio : .mp3, .m4a, .wav, .ogg, .aac, .opus
- AutoCAD : .dwg
- Archives : .zip, .rar, .7z, .rbz, .a
- HAUT : .stl
- Calendrier : .ics
- Code-barres : .btw
- Livre électronique : .azw3, .epub
- Excel : .xlsx, .xls, .xlsm, .ods, .csv, nombres, .xlsb, .gsheet, .xlt, .xltx
- Flash : .swf, .f4v
- Illustrations : .ai, .svg, .skp, .odg, .emf, .wmf, .vsdx, .jpe, .ps, .mcd, .psd, .xcf
- Images : .jpg, .png, .heic, .gif, .jfif, .webp, .ico, .jpeg, .tif, .tiff, .bmp, .wdp, .jxr, .pdn, .jp2
- JSON : .json
- Licence Keynote : .key
- Courrier : .msg, .eml
- Mathematica : .mm
- Rapport Microsoft Power BI : .pbix
- Carte mentale : .xmind, .mvdx
- Modélisation : .rfa, .ifc
- Musique : .enc
- Rapport réseau : .pkt
- Une note : .one
- PDF : .pdf, .xps
- Projet : .gan
- Éditeur : .pub
- Question : .quiz
- Tableau : .déjà
- Texte : .log

- Texte brut : .txt, .md
- Diaporama : .pptx, .ppt, .ppsx, .odp ; .pptm, .ppsm, .pps, gslides, paperboard, .ppta
- Coffre-fort : .dvs
- Vidéo : .wmv, .vob, .mts.mpg, .mpeg, .mkv, .m2ts, .flv, .3gp, .mp4, .webm, .mov, .m4v, .3gpp, .m2t, .avi
- Mot : .docx, .doc, .odt, .pages, .rtf, .story, .dotx, .dot, .wps, .sdoc
- Modules SCORM, version 1.2 ou 2004

Le contenu partageable à partir du Web (lien direct, code d'intégration ou code iframe) peut également être importé, y compris le contenu de services tels que YouTube, Slideshare ou Prezi.

3. Accessibilité

360Learning applique les meilleures pratiques en matière d'expérience utilisateur (UX). Nos équipes Produit et Design se tiennent informées des dernières tendances UX/UI. Nous optimisons l'ergonomie de notre plateforme grâce à des améliorations continues basées sur les données et les retours utilisateurs.

Chez 360Learning, le design est autant un élément de comportement et d'émotion qu'un élément d'utilité et de facilité. C'est pourquoi la convivialité et le design sont au cœur de notre LMS, de notre outil auteur et de nos fonctionnalités sociales et collaboratives.

360Learning s'inspire des normes et recommandations du W3C (World Wide Web Consortium), consortium chargé de promouvoir la compatibilité des technologies Web, et du référentiel RGAA (Référentiel général d'accessibilité pour les administrations). Le RGAA a pour objet de définir les modalités techniques d'accessibilité des services en ligne de l'État en France, ainsi que de ceux des territoires et des établissements publics sous tutelle de l'État, pour les trois canaux que sont l'internet, la télévision et la téléphonie.

Suite à un audit réalisé par Level Access, notre partenaire accessibilité, en janvier 2025, nous sommes partiellement conformes aux WCAG Niveau AA et nous poursuivons nos efforts autour de l'accessibilité.
Ce sont les éléments de conformité sur la plateforme 360Learning :

LISIBILITÉ

- La police utilisée est Open Sans. Une police claire et simple pour une meilleure lisibilité.
- L'utilisation des majuscules est réduite au strict minimum.
- Sous-titres générés automatiquement disponibles sur les vidéos de cours (l'utilisation standard des vidéos s'arrête à 2,5 heures/utilisateur/an)
- 360Learning privilégie les combinaisons de couleurs à fort contraste pour une lisibilité optimale. Par exemple : blanc/noir – bleu foncé/blanc. Nous veillons à ce que la combinaison texte/couleur d'arrière-plan respecte le ratio recommandé de 4,5:1 pour un texte standard (< 19 px) et de 3:1 pour un texte plus grand (=> 19 px).

BARRE DE NAVIGATION

Nous fournissons des barres de navigation standard qui sont toujours au même endroit, nous fournissons également un outil de recherche et des liens de saut.

ZONAGE ET LISIBLE COGNITIVE

La navigation sur 360Learning est semi-guidée.
Chaque zone est distinctement séparée et correspond à une activité.
La structure de chaque cours est la même, permettant à l'utilisateur de simplifier et de mémoriser le chemin de navigation.

ÉLÉMENT D'ORIENTATION UTILISATEUR

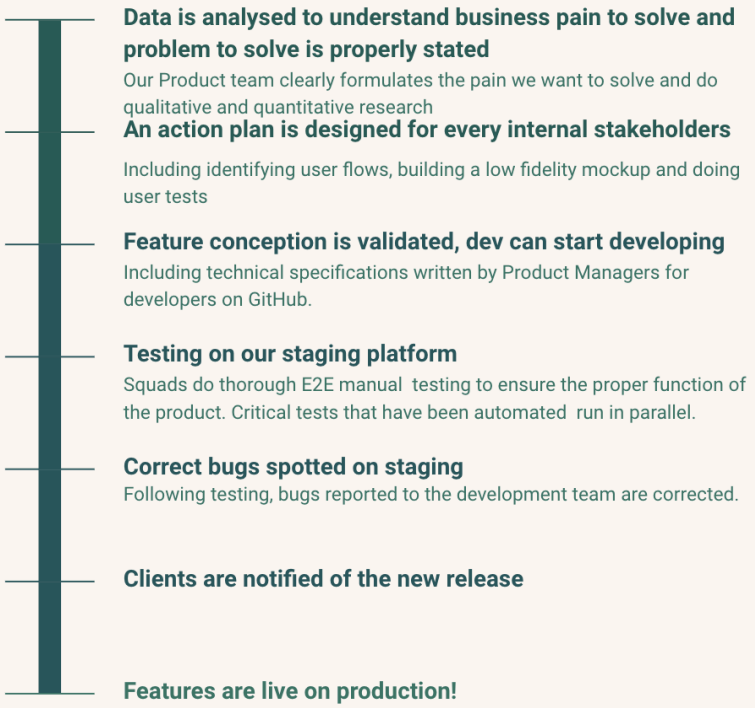
La plateforme permet à l'apprenant de distinguer facilement la page affichée parmi celles du site, à tout moment. L'interface utilisateur propose notamment un élément qui l'aide à déterminer :

- Où ils se trouvent : Le menu correspondant est affiché en gras et est plus lumineux
- D'où ils viennent :L'apprenant peut se situer à tout moment dans le programme(fil d'Ariane)
- Où ils peuvent aller ensuite : L'apprenant peut se projeter dans son parcours

4. Développement

NOUVELLES FONCTIONNALITÉS

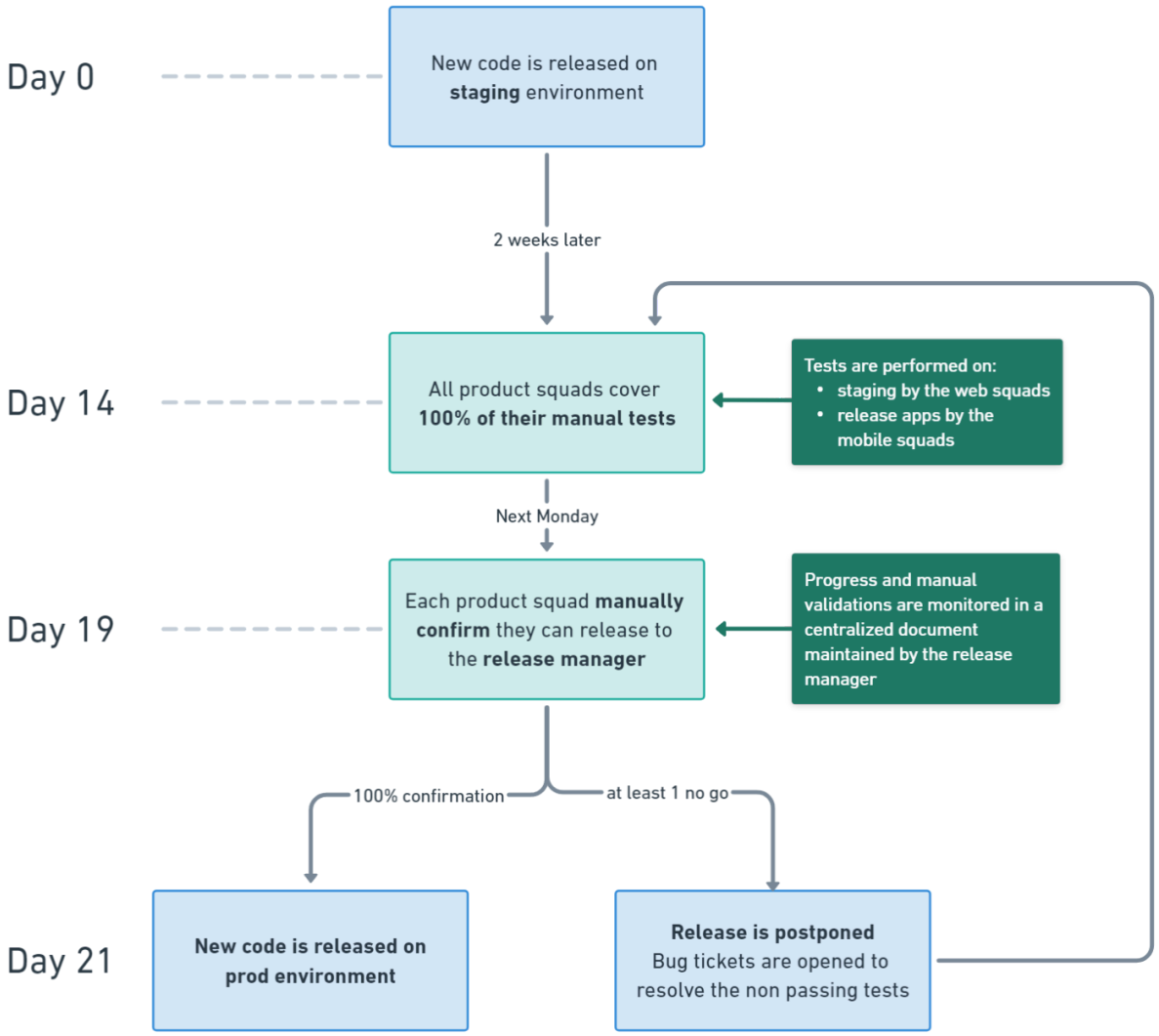
Chaque nouvelle fonctionnalité est développée selon un plan très précis, détaillé ci-dessous.



ASSURANCE QUALITÉ

Chaque fonctionnalité est testée sur un **environnement de préparation** avant son déploiement sur l'**environnement de production**, en suivant le processus détaillé ci-dessous. 👇

Afin de garantir le niveau de qualité attendu des fonctionnalités, sans compromettre les autres fonctionnalités de la plateforme, nous effectuons des tests manuels de bout en bout pour chaque étape. Un responsable de version est désigné et doit garantir le respect de ce processus, notamment en communiquant avec les responsables techniques pendant la phase de déploiement.



Environnement de préparation

Une réplique quasi exacte de notre environnement de production pour les tests logiciels. Nous utilisons l'environnement de test pour tester les builds dans un environnement de production avant le déploiement de l'application.

Environnement de production

C'est là que la dernière version de notre plateforme est disponible pour les utilisateurs. C'est l'environnement où les utilisateurs finaux peuvent voir, expérimenter et interagir avec le produit.

Personnaliser l'apparence de la plateforme avec un CSS personnalisé (paramètre facultatif)

360Learning peut décider d'offrir, à titre commercial et gratuitement, du CSS personnalisé à un client qui en fait la demande. Ce paramètre facultatif ne peut être activé que par le gestionnaire de compte et sous

certaines conditions. Les recommandations générales concernant le CSS personnalisé sont détaillées dans cet article de la base de connaissances 360Learning :https://support.360learning.com/hc/en-us/articles/4956106195732-Personnaliser-l-apparence-de-la-plateforme-avec-des-CSS-personnalisés

Le client est responsable de toutes les modifications apportées aux paramètres de sa plateforme avec du CSS personnalisé. 360Learning n'assure pas la configuration, la maintenance, l'interopérabilité ni le support du code personnalisé. Par exemple, si un client estime que le CSS personnalisé lui convient, les propriétaires de la plateforme doivent être prêts à :

- Testez le code personnalisé à chaque version, qui se produit toutes les 3 semaines.
- Gérez, dépannez et prenez en charge tous les problèmes de code personnalisé.

360Learning : (i) peut désactiver le CSS personnalisé du client à tout moment, en particulier si 360Learning détermine que des problèmes de sécurité ou de performance sont identifiés ; et (iii) ne prend aucune garantie expresse ou implicite d'aucune sorte sur le CSS personnalisé.

Toute utilisation de CSS personnalisé par un client n'autorise pas le client à créer des œuvres dérivées de la plateforme.

Sécurité

1. Cryptage

Par défaut, l'accès à l'application est systématiquement forcé à utiliser HTTPS TLS 1.2 minimum avec un ensemble de chiffrements forts compatibles.

Veuillez vous assurer de la compatibilité de votre système d'information avec cet ensemble de chiffrements :

#TLS 1.2
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh2048)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh2048)
TLS_ECDHE_RSA_AVEC_AES_128_GCM_SHA256 (secp256r1)
TLS_ECDHE_RSA_AVEC_AES_256_GCM_SHA384 (secp256r1)
TLS_ECDHE_RSA_AVEC_CHACHA20_POLY1305_SHA256 (secp256r1)

#TLS 1.3
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

N.B. : Nous maintenons cette liste à jour pour une compatibilité maximale avec les navigateurs web récents, tout en garantissant un niveau de sécurité optimal. La compatibilité ne devrait pas poser de problème, sauf si vous utilisez un navigateur web ancien ou des outils de bibliothèque client http obsolètes.

ACCÈS PROTÉGÉ PAR MOT DE PASSE

L'accès à l'application est protégé par un mot de passe, qui peut être défini de plusieurs manières :

- Par l'utilisateur lors de la première connexion.
- Par un administrateur lors de la création du compte.
- Par le mécanisme SSO, dans ce cas 360Learning stocke une chaîne aléatoire de 32 caractères comme espace réservé pour le mot de passe dans sa base de données.

Une fois ce mot de passe défini, il est impossible pour un tiers d'en prendre connaissance en interrogeant notre base de données, car tous les mots de passe sont hachés de manière irréversible grâce à BCRYPT 10 tours. En cas d'attaque, nous avertirons rapidement tous les clients concernés.

CONTRÔLE D'ACCÈS PAR ADRESSE IP

Il est possible de filtrer l'adresse IP pour contraindre l'accès à l'application : les utilisateurs ne peuvent alors se connecter que depuis un emplacement défini.

2. Sécurité physique

CENTRES DE DONNÉES HAUTEMENT SÉCURISÉS

L'infrastructure principale de 360Learning est hébergée chez notre partenaire Microsoft Azure. Microsoft Azure offre le plus haut niveau de sécurité pour garantir la disponibilité, l'intégrité et la confidentialité des données hébergées.

CARACTÉRISTIQUES DES CENTRES DE DONNÉES – OVH

Sécurité et incendie

- L'accès physique aux serveurs informatiques est limité aux employés accrédités
- Accès contrôlé par badge RFID, installations surveillées par un service de sécurité professionnel 24h/24 et 7j/7
- Systèmes de vidéosurveillance et de détection de mouvement
- Chambres équipées de systèmes de détection de fumée et de chaleur
- OVH s'appuie sur les normes ISO 27002 et ISO 27005 pour la gestion de la sécurité, l'évaluation des risques et les mesures d'atténuation pertinentes.

Alimentation électrique

- Double alimentation systématique
- Onduleurs 250 KVA
- Générateurs avec une autonomie initiale de 48 heures
- Un minimum de 2 flux réseau entrants vers le centre de données ; à l'intérieur, 2 réseaux

Contrôle du climat

- Le watercooling disperse 70 % de la chaleur émise par le processeur
- Le refroidissement par air disperse les 30 % restants
- PUE entre 1 et 1,2 : consommation énergétique des data centers en constante réduction.

jumeaux (salles capables de prendre le relais l'une de l'autre)

Installations	Maintenance et gestion technique des installations
• OVH conçoit et construit son propre centre de données depuis 2003 • Les centres de données d'OVH sont situés en dehors des zones géographiques soumises au Patriot Act • Les installations sont situées à au moins 125 miles les unes des autres afin de garantir la redondance et la continuité du service	• Personnel technique présent sur place 24h/24 et 7j/7

CARACTÉRISTIQUES DES CENTRES DE DONNÉES – Microsoft Azure

Sécurité et incendie
• Contrôle d'accès autonome par badge sans contact RFID, et biométrique par reconnaissance du réseau veineux des doigts • Porte d'entrée blindée à double battant conforme aux normes anti-intrusion EN1627 • Réseaux extérieurs et intérieurs de caméras numériques • Dispositifs anti-intrusion sur tous les points d'accès (APSAD R81) et APSAD R81 (détection d'intrusion) • Agent de sécurité incendie avec spécialisation SSIAP 2, sur site 24h/24 et 7j/7 • Systèmes de détection multipoints VESDA LASER • Systèmes d'extinction d'incendie par brouillard d'eau SEMCO conformes aux normes APSAD R1/D2 et NFPA 750 • Moyens de lutte contre l'incendie RIA supplémentaires et extincteurs portables au CO2 conformes aux normes APSAD R4 • Compartiment coupe-feu entre chaque salle informatique capable de résister au feu pendant deux heures

Alimentation électrique

- Entrée du réseau électrique EDF via 2 sorties T bidirectionnelles de 9 MVA chacune
- 7 tableaux principaux de distribution basse tension I de 2,5 MVA chacun, équipés d'un dispositif de commutation automatique vers un appareil de redondance du générateur
- 6 générateurs au gazole pour une puissance installée de 11,85 MVA
- 48 800 litres de fioul, 50 heures d'autonomie à pleine charge
- Zone N+1 : 3 circuits UPS indépendants
- Zone 2(N+1) : 2 circuits UPS indépendants
- Autonomie de la batterie : 10 minutes en fin de vie de la batterie

Contrôle du climat

- 5 MW de capacité de refroidissement en configuration N+1
- Réseau d'eau glacée redondant via des boucles (circuits de distribution)
- Armoires climatiques de 90 kW
- Température maintenue à 20°C +/-2°C en allée froide
- Aménagement systématique d'allée froide confinée
- Climatisation indépendante pour chaque chambre client

Installations

- Conception et construction spécifiquement conçues pour être utilisées comme centre de données

Maintenance et gestion technique des installations

- Maintenance conforme aux normes AFNOR NF EN 13-306 et FD X60-000
- Surveillance à distance des équipements par les fabricants
- Gestion des infrastructures par GTC Sima©

CARACTÉRISTIQUES DES CENTRES DE DONNÉES – AWS

Sécurité et incendie

- L'accès physique aux serveurs informatiques est limité aux employés accrédités
- Accès contrôlé multifactoriel, installations surveillées par un service de sécurité professionnel 24h/24 et 7j/7
- Les accès physiques aux salles de serveurs sont enregistrés par caméra de vidéosurveillance. Les images sont conservées conformément aux exigences légales et réglementaires.
- Chambres équipées de systèmes de détection de fumée et de chaleur
- Les tests tiers des centres de données AWS, tels que documentés dans nos rapports tiers, garantissent qu'AWS a mis en œuvre de manière appropriée des mesures de sécurité alignées sur les règles établies nécessaires pour obtenir des certifications de sécurité.

Alimentation électrique

- Les systèmes d'alimentation électrique des centres de données AWS sont conçus pour être entièrement redondants et maintenables sans impact sur les opérations, 24 h/24. AWS veille à ce que les centres de données soient équipés d'une alimentation de secours afin de garantir la disponibilité de l'électricité nécessaire au maintien des opérations en cas de panne électrique des charges critiques et essentielles de l'installation.

Contrôle du climat

- Les centres de données AWS utilisent des mécanismes de contrôle climatique et maintiennent une température de fonctionnement adéquate pour les serveurs et autres équipements afin d'éviter toute surchauffe et de réduire les risques de pannes de service. Le personnel et les systèmes surveillent et maintiennent la température et l'humidité à des niveaux appropriés.

Installations

- AWS conçoit et construit ses propres centres de données
- Les centres de données d'AWS traitent les données des centres de données de l'UE sur lesquels nous comptons.
- Les installations sont situées à au moins 125 miles les unes des autres afin de garantir la redondance et la continuité du service

Maintenance et gestion technique des installations

- Des systèmes électroniques de détection d'intrusion sont installés au sein de la couche de données pour surveiller, détecter et alerter automatiquement le personnel concerné en cas d'incident de sécurité. Les points d'entrée et de sortie des salles de serveurs sont sécurisés par des dispositifs exigeant une authentification multifacteur pour chaque personne avant d'autoriser l'entrée ou la sortie.

3. Sécurité logique

Voici un bref résumé de nos éléments de sécurité. Pour plus de détails, veuillez consulter notre Plan d'assurance de sécurité v3.3.

PRÉVENTION DES ATTAQUES PAR DÉNI DE SERVICE (DDOS)

Une attaque DDoS vise à rendre votre site indisponible en surchargeant la bande passante du serveur ou en occupant ses ressources jusqu'à leur épuisement. Les cas rencontrés sont généralement des attaques de niveau 7 (le plus élevé), basées sur l'exécution d'un grand nombre de requêtes afin de saturer le système.

Garantir la sécurité en ligne de ses clients et la disponibilité de ses services est au cœur des préoccupations de 360Learning. Afin de contrer ces attaques, notre hébergeur Microsoft Azure adopte en standard une solution de mitigation basée sur la technologie VAC. Celle-ci repose sur une combinaison exclusive de techniques qui analysent votre trafic en temps réel et à grande vitesse. Elles détectent et interceptent automatiquement les attaques tout en laissant passer les requêtes légitimes.

DÉTECTION ET PRÉVENTION DES ATTAQUES OWASP

Un pare-feu applicatif web de nouvelle génération, installé sur nos serveurs frontaux, filtre chaque requête pour identifier toute menace potentielle. Il intègre la détection OWASP classique et des règles métier spécifiques pour alerter et bloquer les tentatives malveillantes.
Des alertes sont envoyées au DevOPS et à l'équipe de sécurité pour lancer si nécessaire un incident de sécurité.
Toutes les attaques sont enregistrées et conservées au moins 6 mois pour garantir des audits de sécurité appropriés.

ANTIVIRUS

Notre solution privilégiée est la dernière version de la suite d'outils ClamAV. Elle est mise à jour automatiquement toutes les 60 minutes afin de garantir l'utilisation constante de la base de données la plus récente pour la détection et la prévention des menaces. Une analyse est effectuée sur tous les fichiers et archives téléchargés afin de garantir l'absence de fichiers exécutables.

Si un virus est détecté, l'utilisateur qui tente de l'importer est averti par ce message : « Votre document semble suspect pour notre antivirus. Votre fichier n'a pas été importé. » Et le fichier n'est jamais importé.

DÉTECTION ET RÉPARATION DES MENACES

Nous avons déployé :

- Une solution de détection et de réponse aux points d'extrémité (EDR/XDR) Crowdstrike est installée sur chaque serveur pour garantir une protection élevée et la capacité d'identifier les menaces sur notre plateforme (ransomwares, malwares, rootkits, shell distant, etc.). Chaque agent est connecté à une plateforme centrale, gérée en externe 24h/24 et 7j/7 par les équipes CrowdStrike, qui transmettent l'alerte à l'équipe de sécurité interne de 360Learning en cas d'urgence.
- un pare-feu d'application Web de nouvelle génération qui filtre chaque requête pour toutes nos applications et points de terminaison externes.
- Un SIEM corrélant les logs de l'ensemble de notre entreprise et de notre plateforme. Il est accompagné d'un SOC externe, disponible 24h/24 et 7j/7, qui alerte l'équipe de sécurité en cas de comportement anormal (non-conformité, attaque, comportement inhabituel comme une authentification réussie provenant d'une source inconnue).

RÔLES AU SEIN DE L'APPLICATION

La plateforme prend en charge plusieurs rôles et ensembles d'autorisations granulaires, ce qui nous permet d'appliquer une politique de contrôle d'accès bien adaptée en fonction du rôle de chaque utilisateur.

Les rôles déterminent ce que les utilisateurs peuvent voir et faire dans 360Learning. Les rôles principaux définissent le niveau d'accès dont disposent les utilisateurs pour gérer les comptes, le contenu de formation et les paramètres dans 360Learning (accès administrateur). Des rôles spécifiques donnent accès à davantage de fonctionnalités collaboratives dans 360Learning.

RÔLES PRINCIPAUX

Apprenant

Les apprenants ont accès aux pages d'accueil de leurs groupes, peuvent lire du contenu de formation partagé par les auteurs, les coachs et les administrateurs et peuvent utiliser les fonctionnalités sociales de la plateforme.
Les apprenants n'ont pas d'accès administrateur.

Les droits des apprenants comprennent :

- Accès au contenu de formation
- Possibilité de publier des messages dans des groupes et des forums de contenu de formation
- Accès à leurs analyses d'apprentissage personnelles

Auteur

Les auteurs peuvent créer du contenu de formation et partager du contenu avec la bibliothèque de leur groupe.

Les droits d'auteur incluent :

- Capacité à créer du contenu de formation (cours, modèles de programmes, sessions de programmes, parcours et sessions de parcours).
- Possibilité d'ajouter des cours, des modèles de programmes et des chemins à la bibliothèque du groupe.
- Capacité à créer des compétences.
- Possibilité d'accéder aux statistiques de leur contenu de formation.

Entraîneur

Les coachs peuvent consulter et exporter les statistiques de leur groupe et partager le contenu de formation avec leur groupe.

Les droits de l'entraîneur incluent :

- Possibilité de regarder n'importe quelle formation depuis la bibliothèque de leur groupe
- Possibilité de créer des sessions à partir de modèles de programmes dans la bibliothèque du groupe
- Accès aux statistiques d'entraînement du groupe depuis le menu Tableau de bord
- Possibilité d'ajouter le groupe à une nouvelle session
- Possibilité d'envoyer des rappels

Administrateur des utilisateurs

Les administrateurs utilisateurs peuvent ajouter et supprimer des utilisateurs de leur groupe et effectuer d'autres actions de gestion des utilisateurs.

Les droits d'administrateur utilisateur incluent :

- Possibilité d'inviter ou d'ajouter directement des apprenants dans leur groupe
- Possibilité d'annuler les invitations de leur groupe
- Possibilité de valider les inscriptions envoyées par les coachs de groupe (si l'option de validation est activée)

Administrateur de groupe

Les administrateurs disposent d'un accès complet à leurs groupes. Ils disposent également des mêmes droits que les auteurs, les coachs et les administrateurs utilisateurs.

Les droits d'administrateur incluent :

- Possibilité de modifier les paramètres du groupe
- Possibilité de valider les inscriptions envoyées par les coachs de groupe (si l'option de validation est activée)

Administrateur de la plateforme

Les administrateurs de la plateforme disposent d'un accès administrateur complet à tous les groupes et d'un accès administrateur complet à la plateforme, y compris :

- Possibilité de configurer la chaîne publique (si nommé administrateur du groupe de la plateforme à l'échelle de l'entreprise)
- Accès aux paramètres avancés de la plateforme (si nommé administrateur du groupe à l'échelle de l'entreprise)
- Accès à la création de badges (si nommé administrateur du groupe à l'échelle de l'entreprise)

Propriétaire

Les plateformes ont un seul propriétaire. Ce dernier dispose des mêmes droits que les administrateurs et est le seul à pouvoir accéder au menu de facturation.

Les droits du propriétaire comprennent :

- Toutes les autorisations d'administrateur de la plateforme
- Accès aux informations de facturation
- Téléchargez toutes les données de la plateforme au format JSON

RÔLES SPÉCIFIQUES

Auteur principal

L'auteur principal d'un cours ou d'un parcours peut le modifier et accéder à sa page de statistiques. Un seul utilisateur peut être l'auteur principal ; vous pouvez le modifier, et ses autorisations sont transférées lors de sa suppression de la plateforme.

Les principaux droits d'auteur incluent :

- Possibilité d'éditer le contenu de la formation.
- Possibilité d'accéder aux statistiques du contenu de la formation

Instructeur

Les instructeurs sont en charge des séances de programme et des séances de parcours.

Les droits de l'instructeur incluent :

- Accédez aux statistiques de leur parcours et des séances de leur programme.

- Réception des notifications liées au programme (informations de connexion, commentaires, publications, programme terminé)
- Correction des questions ouvertes
- Correction des étapes d'évaluation
- Gestion des participants à la session (ajouter/supprimer des participants à la session)
- Possibilité d'envoyer des rappels à partir des statistiques de session

Directeur

Les gestionnaires peuvent accéder aux statistiques d'un utilisateur (même sur les cours ou sessions auxquels ils ne peuvent pas accéder eux-mêmes).

Les gestionnaires peuvent :

- Accédez aux statistiques de leurs managers depuis le menu Tableau de bord
- Recevez un e-mail hebdomadaire présentant les progrès de leurs managers (ils peuvent désactiver cette option dans leurs paramètres)
- Étapes d'évaluation correctes

Co-auteur (cours ou parcours)

Les co-auteurs de cours et de parcours ont les mêmes autorisations qu'un auteur principal, mais leurs autorisations ne sont pas transférées lorsqu'ils sont supprimés de la plateforme.

Les co-auteurs peuvent :

- Modifier les cours et les parcours

Critique

Les réviseurs peuvent évaluer les cours et publier des commentaires internes sur le forum de ces cours. Ce rôle est disponible uniquement avec la solution Champion.

Les évaluateurs peuvent :

- Publier des commentaires internes dans un cours

PARE-FEU ET FILTRAGE DE PORT

Les pare-feu sur les serveurs de 360Learning offrent un niveau de sécurité supplémentaire en matière de contrôle de flux. Tous les ports non essentiels au fonctionnement et à l'administration de la plateforme sont fermés.
Nous utilisons un outil de gestion de la posture de sécurité du Cloud pour alerter en cas d'ouverture d'un port non conforme à notre politique de sécurité.

4. Politiques internes

POLITIQUE DE SÉCURITÉ DES MOTS DE PASSE

1.Aperçu

Tous les employés et le personnel ayant accès aux systèmes informatiques de l'organisation doivent adhérer à notre charte informatique et aux politiques de mots de passe définies ci-dessous afin de protéger la sécurité du réseau, l'intégrité des données et les systèmes informatiques.

2.But

Cette politique est conçue pour protéger les ressources organisationnelles sur le réseau en exigeant des mots de passe forts ainsi qu'une protection de ces mots de passe et en établissant un délai minimum entre les modifications des mots de passe.

3.Portée

Cette politique s'applique à tout le personnel disposant d'un compte informatique nécessitant un mot de passe sur le réseau organisationnel, y compris, mais sans s'y limiter, un compte de domaine et un compte de messagerie électronique.

4.Protection par mot de passe

- N'écrivez jamais vos mots de passe
- N'envoyez jamais de mot de passe par e-mail
- N'incluez jamais de mot de passe dans un document stocké non chiffré
- Ne révélez jamais votre mot de passe à personne
- Ne révélez jamais votre mot de passe par téléphone
- Ne faites jamais allusion au format de votre mot de passe
- Ne révélez jamais ou ne laissez jamais entendre votre mot de passe sur un formulaire sur Internet
- N'utilisez jamais la fonction « Mémoriser le mot de passe » des programmes d'application tels que votre programme de messagerie ou tout autre programme.
- N'utilisez jamais votre mot de passe d'entreprise ou de réseau sur un compte sur Internet qui ne dispose pas d'une connexion sécurisée où l'adresse du navigateur Web commence par https:// plutôt que http://
- Utilisez toujours notre gestionnaire de mots de passe officiel
- Signalez tout soupçon de compromission de votre mot de passe à votre service de sécurité informatique.
- Si quelqu'un vous demande votre mot de passe, orientez-le vers votre service de sécurité informatique.
- Soyez prudent et ne laissez personne vous voir taper votre mot de passe.
- Utilisez l'authentification multifacteur autant que possible

5.Application de la loi

Étant donné que la sécurité des mots de passe est essentielle à la sécurité de l'organisation et de tous, les employés qui ne respectent pas cette politique peuvent faire l'objet de mesures disciplinaires pouvant aller jusqu'au licenciement.
Afin de garantir le niveau de sensibilisation de nos employés, nous menons régulièrement des campagnes de phishing, des formations et des quiz.

6. Autres considérations

Les économiseurs d'écran protégés par mot de passe doivent être activés et protéger l'ordinateur pendant 10 minutes d'inactivité. Les ordinateurs ne doivent pas être laissés sans surveillance lorsque l'utilisateur est connecté et qu'aucun économiseur d'écran protégé par mot de passe n'est actif. Les utilisateurs doivent prendre l'habitude de ne pas laisser leur ordinateur déverrouillé.

Les mots de passe administrateur doivent être soigneusement protégés. Les comptes administrateur doivent disposer d'un accès minimal pour exercer leurs fonctions. Ils ne doivent jamais être partagés.

7. Utilisation d'un portefeuille de mots de passe

L'utilisation d'un gestionnaire de mots de passe, 1Password dans notre cas, facilite les points mentionnés ci-dessus.

Qu'est-ce que cela apporte ?

- Il n'y a qu'un seul mot de passe principal à retenir.
- Il permet de partager l'accès à un compte de manière sécurisée sans donner le mot de passe.
- Il permet la génération de mots de passe sécurisés.

Comment ça marche ?

- Cryptage AES 256 bits avec itérations PBKDF2 régulièrement augmentées
- Toutes les données sensibles sont chiffrées et déchiffrées localement avant d'être synchronisées avec 1Password. La clé reste toujours sur l'appareil et n'est jamais partagée avec 1Password. Nos données restent accessibles uniquement à nous.

5. Sécurité des applications mobiles

- Notre application utilise les mêmes serveurs que notre client Web et se connecte également via HTTPS avec TLS 1.2 (TLS 1.3 et bénéficie ainsi des mêmes niveaux de sécurité. Ainsi, les journaux sont conservés et traités de la même manière, qu'ils soient générés à l'aide de l'application mobile ou de l'application Web.
- De même, si vous imposez l'acceptation d'une Politique de confidentialité, les utilisateurs devront l'accepter dès leur première connexion, quel que soit le client utilisé (mobile ou web).
- Les données de géolocalisation sont pseudonymisées lors de la collecte à des fins d'analyse de produit, de sorte qu'aucune donnée personnelle n'est enregistrée lors de l'utilisation de notre application.
- Que ce soit sur iOS ou Android, les données hors ligne ne sont en aucun cas accessibles par une autre application ou directement avec le système d'exploitation.
- Nos applications mobiles sont soumises à des tests de pénétration une fois par an.

6. Audits indépendants

HDWSEC, HACKERONE, NeverHack : Expert en sécurité en collaboration avec 360Learning

HDWsec, auditeur et expert indépendant français en sécurité, intervient aux côtés de 360Learning sur la gestion de la sécurité de son infrastructure logicielle et réseau, ainsi que sur la mise en œuvre de sa politique de sécurité.
HackerOne est un célèbre spécialiste américain indépendant des tests de pénétration qui garantit des tests de vulnérabilité plus approfondis et des programmes détaillés pour garantir une sécurité et une conformité maximales.

Afin d'évaluer et de renforcer la sécurité de 360Learning, HDWsec réalise :

- 1 audit de sécurité par an, suivant la méthodologie OWASP avec tests greybox et blackbox, incluant un audit complet de la configuration de l'architecture de 360Learning et des attaques simulées (tentatives de piratage)
- Formation continue à la sécurité des développeurs 360Learning
- Conseil dans la mise en œuvre de la politique de sécurité de 360Learning

Afin de maximiser la connaissance de la vulnérabilité et de la conformité de la sécurité de 360Learning, HackerOne réalise :

- 1 audit de pentest de sécurité programmé approfondi par an avec des hackers spécifiquement choisis pour leur connaissance de nos technologies.
- Contrôle continu de conformité

Afin d'évaluer le niveau global de sécurité de l'entreprise, NeverHack mène un exercice Red Team sur l'ensemble des actifs de l'entreprise, en essayant de recueillir des informations sur :

- faux e-mails

- faux appels téléphoniques
- nos outils d'entreprise
- nos infrastructures
- nos applications

7. Normes

Nom légal des sous-traitants				
Microsoft Azure	✅	✅	🚫	✅
OVH	✅	✅	🚫	✅
AWS	✅	✅	🚫	✅
Scaleway	✅	✅	🚫	✅
Amplitude	✅	✅	🚫	✅
Pendo Inc.	❌	✅	🚫	❌
Gainsight Inc.	❌	✅	🚫	✅
Datadog	✅	✅	🚫	✅
Zendesk	✅	✅	🚫	✅
Stripe (pour les paiements d'offres d'équipe)	✅	✅	✅	❌
Snowflake Computing Pays-Bas B.V.	✅	✅	🚫	✅
Elastic App Search	✅	✅	🚫	✅
Workato	❌	✅	🚫	❌

✅ : Oui

❌: Non
🚫: N/A

Continuité de service

1. Politiques internes

Nous garantissons à tous nos clients un taux **de disponibilité mensuelle de 99,8 %.**

Vous trouverez plus d'informations sur notre SLA à l'adresse suivante :

- Pour les clients Essential et Advanced :[FR]SLA
- Pour les clients Ultimate :https://360learning.com/legal/slaenultimate/

2. Sauvegardes

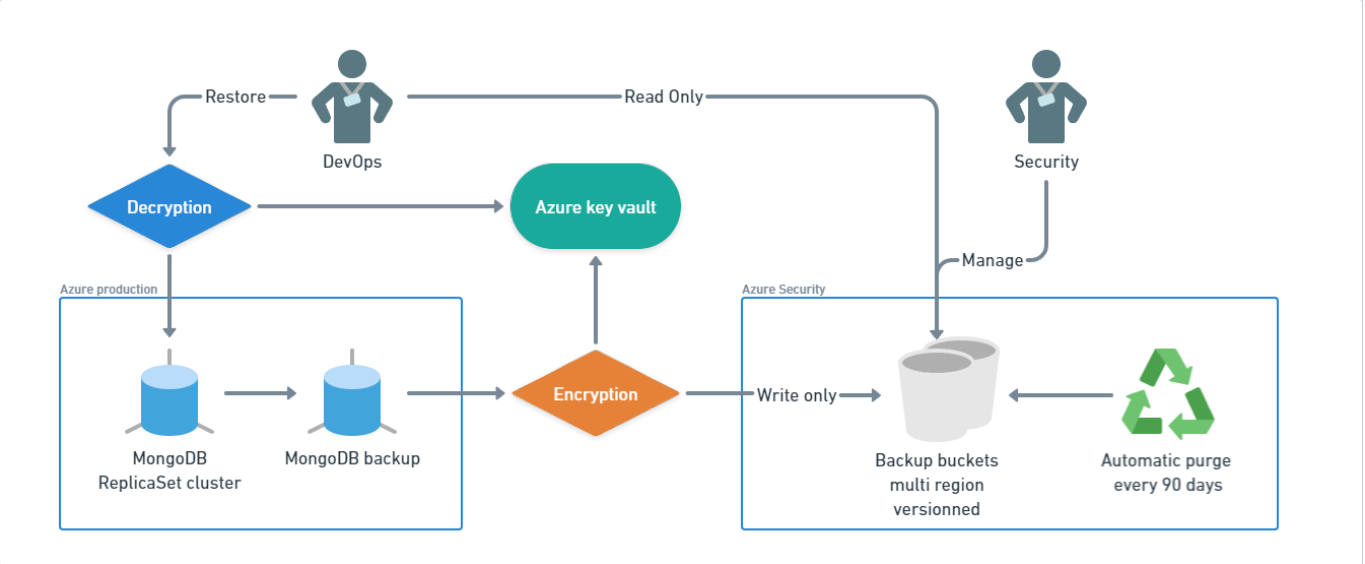
Vos données personnelles ainsi que vos vidéos, images et documents téléchargés sur 360Learning sont hébergés par notre partenaire Microsoft Azure, dans l'un des Data Centers indiqués dans le tableau ci-dessous.

Région	Centre de données Azure	Emplacement physique	Zones de disponibilité	Disponibilité commerciale
France	France Centre	région parisienne	3	Disponible pour tous les clients
États-Unis	US-WEST-2	État de Washington	3	Disponibilité générale prévue en 2024

Pour les autres contenus de formation, des services tiers tels que Youtube, Prezi ou Vimeo sont hébergés par leurs éditeurs.

Les zones de disponibilité Azure sont des emplacements physiquement distincts au sein de chaque région Azure, tolérants aux pannes locales. Ces pannes peuvent aller des pannes logicielles et matérielles aux événements tels que les tremblements de terre, les inondations et les incendies. Cette tolérance aux pannes est obtenue grâce à la redondance et à l'isolation logique des services Azure. Pour garantir la résilience, au moins trois zones de disponibilité distinctes sont présentes dans toutes les régions où elles sont activées..

Les sauvegardes logiques (version du service et données client) sont effectuées une fois par jour sur le cluster de sauvegarde à distance. Cela garantit un RPO maximal de 24 heures, et nous conservons un historique instantané de 90 jours.



3. Redondance

Les serveurs sont répliqués. Les centres de données sont alimentés par deux alimentations indépendantes et équipés d'onduleurs. Des générateurs d'une autonomie de 48 heures garantissent la continuité de la production d'électricité en cas de panne du réseau électrique. Plusieurs boucles de sécurité ont ainsi été mises en place afin d'éviter toute indisponibilité potentielle. Cette multiplicité de liaisons permet également à vos données d'emprunter le chemin le plus court et donc de subir les plus faibles latences. Les serveurs sont également équipés d'une double alimentation et de deux cartes réseau pour une infrastructure entièrement redondante.

4. Reprise du service

PLAN DE REPRISE APRÈS SINISTRE

Le PRA (Plan de Reprise d'Activité) est activé en cas de sinistre impactant l'intégrité des données :

- Défaut logique majeur
- Destruction physique des installations d'hébergement

Dans ce cas, le client est immédiatement averti et la procédure de récupération démarre. La nouvelle infrastructure est recréée dans un centre de données disponible sur Microsoft Azure. Les données sont restaurées à partir de la dernière version des données sauvegardées. Comme indiqué précédemment, les

sauvegardes complètes (version du service et données client) sont effectuées, stockées et chiffrées quatre fois par jour sur un stockage distant ; les données ne quittent jamais physiquement leur emplacement de stockage. Cela garantit un objectif de point de récupération (RPO) maximal de 6. heures.

La durée maximale du PRA est de 12 heures. En cas de changement de centre de données nécessitant une modification des adresses IP des entrées DNS, la mise à jour des caches DNS dans le monde entier ne prend pas plus de 24 heures.

Cela garantit un RTO (Recovery Time Objective) inférieur à 24 heures.
Pour des informations plus détaillées, veuillez vous référer au document nommé :

RÉPONSE EN CAS D'INCIDENT

Chez les hôtes de 360Learning

Les alarmes sont configurées pour avertir automatiquement les équipes opérationnelles dès que les premiers signes d'alerte atteignent des seuils prédéfinis. Une fois le seuil atteint, la réponse aux incidents DevOps est activée.

Microsoft Azure met en place des systèmes de journalisation et de reporting en temps réel afin d'enregistrer et de signaler les événements liés à la sécurité.

Tous les événements sont documentés et enregistrés pendant une période de 90 jours après qu'ils ont été observés.

Sur notre réseau

360Learning utilise un système de jeton unique associé à l'adresse IP pour garantir qu'aucun intrus ne puisse intercepter les échanges et communiquer avec l'API à la place de l'utilisateur (attaques de type « man-in-the-middle »). Toute tentative de connexion de ce type est refusée et enregistrée. En cas d'attaque détectée, tous les clients concernés sont avertis sous 24 heures.

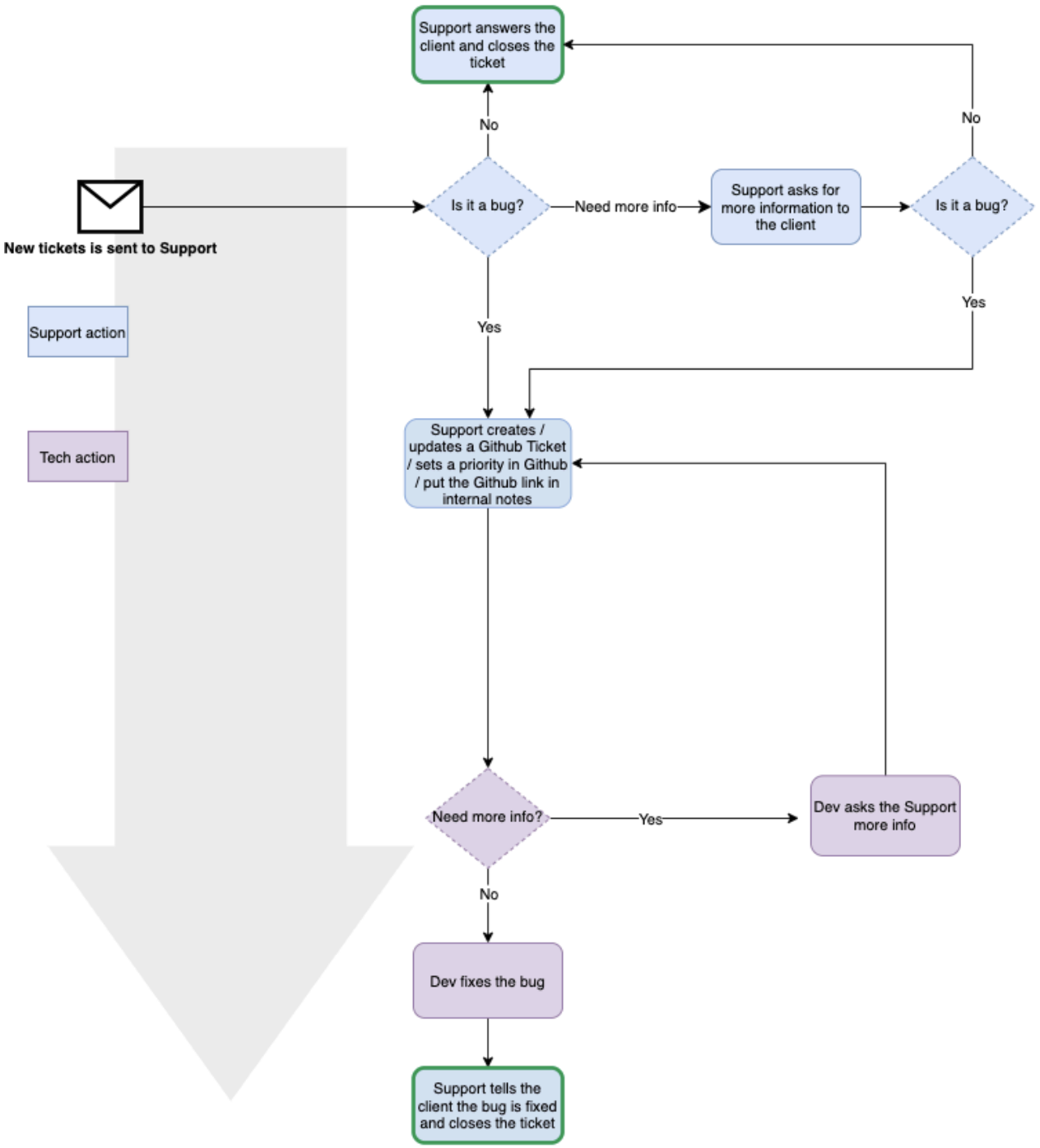
SUPPORT TECHNIQUE

360Learning propose un service d'assistance technique en ligne, accessible en français, anglaiset en allemand pendant les heures d'ouverture : de 9h00 à 18h00 (heure d'Europe centrale), du lundi au vendredi.

- Support technique et fonctionnel avec Zendesk
- Fourniture d'aide contextuelle en ligne
- Support dans l'utilisation de l'API documentée
- Prise en charge des intégrations SSO

PROCESSUS DE SOUTIEN

Ticket funnel



Évolutivité

1. Occupation du système

SAAS (LOGICIEL EN TANT QUE SERVICE)

360Learning propose un logiciel de type SaaS (Software as a Service). Le modèle SaaS repose sur l'installation du logiciel sur des serveurs plutôt que sur le poste de travail de l'utilisateur.

Il ne nécessite donc aucune installation et est accessible depuis n'importe quel ordinateur connecté à Internet.

Le modèle SaaS offre une grande flexibilité et permet des mises à jour fréquentes, permettant aux clients de 360Learning de bénéficier à tout moment des dernières avancées technologiques.

ARCHITECTURE LOGICIELLE

Notre architecture est composée de trois couches :

- L'interface, en JavaScript, est exécutée côté client. Elle contient quelques workflows et une logique métier. Cet élément est évolutif naturellement : chaque client le reçoit dès qu'il le souhaite.

se connecte au site et l'exécute lui-même.

Pour obtenir des données à afficher et envoyer de nouvelles données à la plateforme, cette partie envoie des requêtes AJAX à une API REST.

- L'API REST, exposée par un serveur web Node.js, est composée de micro-unités élémentaires (par exemple, une « route » indépendante de toutes les autres au sein de l'API pour ajouter un utilisateur à un programme) que le code client peut appeler. Ces routes contiennent des couches métier parfaitement optimisées et n'utilisent actuellement que 30 % des ressources CPU et 10 % des ressources RAM (un record).
-
- Nœud.jsIl envoie ensuite des requêtes à une base de données MongoDB pour stocker les données. Une seule réplique suffit actuellement à répondre à toutes les requêtes de lecture et d'écriture, consommant environ 10 % de ses ressources. Une fois 40 % des ressources utilisées, un processus de migration sera lancé pour héberger cette base de données MongoDB dans le cloud, en utilisant l'une des trois méthodes de partitionnement standard de MongoDB (le choix sera effectué en fonction de notre profil de charge au moment de la décision de migration). Cette étape standard ne nécessite que quelques lignes de code.configuration.

SURVEILLANCE

360Learning suit les performances de ses serveurs en temps réel afin de garantir la disponibilité de l'architecture. Dès que les performances diminuent et passent sous un seuil critique, un système d'alerte par e-mail informe la direction et le département R&D.

Les indicateurs de performance système surveillés par 360Learning sont le processeur, la RAM, l'utilisation du disque, les E/S, le réseau, le nombre de requêtes, la latence par service et d'autres indicateurs standards. Outre ces indicateurs de base, 360Learning surveille également des indicateurs métier généraux, tels que le nombre de cours suivis, le nombre de ressources créées (cours, utilisateurs, groupes, parcours, etc.), etc. Il n'est pas prévu que les clients y aient accès. 360Learning fournit toutefois des statistiques en temps réel sur l'activité des utilisateurs sur les plateformes de ses clients via le tableau de bord de l'application, qui peut être exporté.

360Learning collecte et stocke les journaux d'accès et de demandes, ainsi que les erreurs et les incidents. Ces données sont stockées, signées et agrégées pour l'ensemble de notre infrastructure et pour tous nos clients. La durée de conservation est fixée à 3 mois minimum et 6 mois maximum.

TECHNOLOGIES ET OUTILS

360Learning utilise des technologies de pointe, adoptées également par les agents les plus importants du Web. Parmi celles-ci :

JavaScript et TypeScript

La plateforme 360Learning est entièrement développée en JavaScript. Elle offre de nombreux avantages :

- Le temps de développement est considérablement réduit : l'équipe R&D ne doit maîtriser qu'une seule technique.
- Les temps de chargement sont optimisés : la charge est déplacée vers le poste de travail de l'utilisateur, qui ne demande les données que lorsque cela est nécessaire.

Pour une fiabilité encore meilleure, le code est actuellement en cours de migration vers TypeScript, un sur-ensemble de JavaScript qui vise à détecter les erreurs et incohérences dans le code avec plus de précision et offre une maintenance plus aisée (plus de 80% des fichiers de code source sont en TypeScript à la date de rédaction).

Vue.js

L'application cliente web 360Learning utilise Vue.js, une bibliothèque JavaScript front-end pour la création d'interfaces utilisateur. Grâce au rendu déclaratif et à la composition de composants, les applications basées sur Vue.js sont beaucoup plus modulaires, extensibles et faciles à maintenir.

Node.js

360Learning utilise Node.js, une plateforme logicielle open source événementielle conçue pour les applications réseau nécessitant une évolutivité. Node.js permet la création d'applications très rapides.

Express.js
Express.js est un framework Node.js qui permet d'exposer une API en toute sécurité.

MongoDB
360Learning utilise MongoDB, un système de gestion de base de données orienté document, une technologie de pointe et évolutive. C'est l'un des SGBD les plus utilisés aujourd'hui, notamment par Facebook, LinkedIn, Google ou Amazon.

Des systèmes de bases de données plus spécialisés
Pour des fonctionnalités spécifiques, 360Learning exploite la puissance de systèmes de gestion de données de pointe plus adaptés, comme ElasticSearch, Redis et Snowflake. Ces systèmes prennent en charge des fonctionnalités telles que les tableaux de bord, Live Learners, Recommendations For You, la recherche, et bien plus encore.

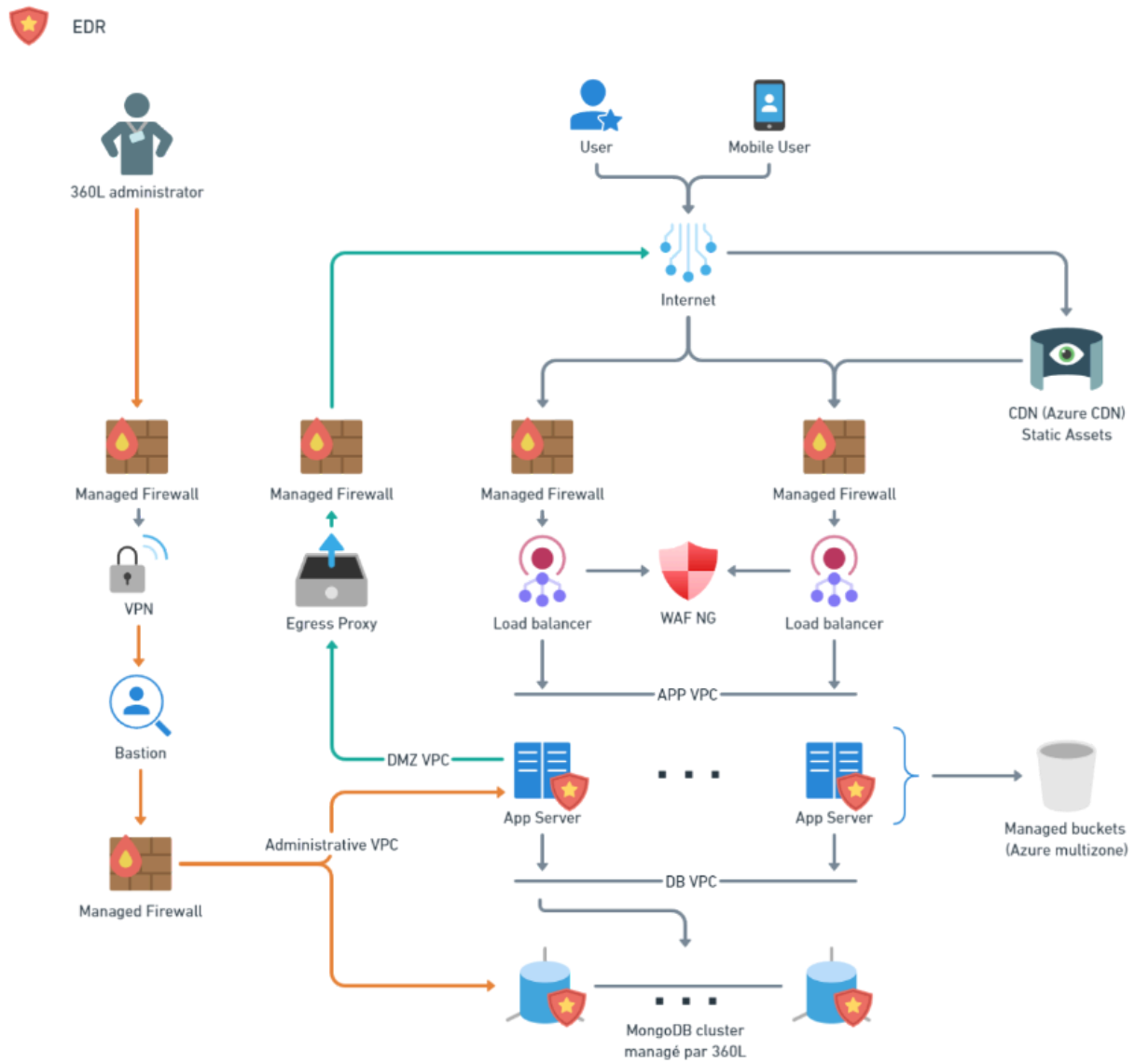
SERVEURS

Le système d'exploitation de nos serveurs est Linux Ubuntu 24.04 LTS.

POLITIQUE DE GESTION DES NOUVELLES VERSIONS DE NAVIGATEURS

Lorsqu'une nouvelle version importante d'un navigateur est publiée, 360Learning s'assure que sa plateforme est compatible.

RÉSEAU



Toutes les données sont répliquées sur un serveur de préproduction, testé en profondeur toutes les trois semaines. Les temps de réponse du cloud sont régulièrement testés avec cinq requêtes prédéfinies. Les temps de réponse depuis la France doivent être inférieurs à 50 ms.

2. Volume de clients

Afin de garantir une utilisation équitable pour tous les utilisateurs, 360Learning documente et, le cas échéant, impose des limites à certaines fonctionnalités. Si le client a besoin de plus de 200 000 utilisateurs pour sa plateforme, l'équipe R&D doit en être informée un mois à l'avance afin de pouvoir

engager un processus de redimensionnement.Une plateforme ne peut pas dépasser 30 000 groupes. Nous appliquons également des limites de taux à l'API 360Learning. De plus, les limites de certaines fonctionnalités sont documentées dans la Base de connaissances 360Learning.

Intégrations

1. SSO

OBJECTIFS

L'authentification unique (SSO) est un mécanisme d'authentification qui permet aux utilisateurs d'accéder à plusieurs applications avec un seul ensemble d'informations de connexion.

En activant le SSO pour votre application 360Learning, vous devenez responsable de l'authentification de vos utilisateurs : ils s'authentifient via votre propre portail de connexion et n'ont plus besoin d'un ensemble supplémentaire de login/mot de passe.
Les avantages de l'utilisation de ce SSO incluent :

- Expérience utilisateur améliorée
- Sécurité améliorée
- Navigation fluide

TECHNOLOGIES

360Learning prend actuellement en charge trois implémentations SSO : JWT (JSON Web Token), SAML (Secure Assertion Markup Language) et OIDC (OpenID Connect).

- SAML est un format plus ancien, basé sur XML. Il est pris en charge par de nombreux services et s'intègre facilement à votre système d'authentification d'entreprise, par exemple Windows Active Directory.

- JWT est une norme assez récente basée sur JSON utilisée dans les derniers protocoles d'authentification.Il offre une grande flexibilité.

- OpenID Connect est basé sur le protocole OAuth 2.0 et utilise un jeton Web JSON (JWT) supplémentaire pour standardiser les domaines que OAuth 2.0 laisse au choix, tels que les étendues et la découverte de points de terminaison.

DOCUMENTATION

Des guides techniques sont disponibles pour les deux technologies pour vous aider à intégrer SSO :

- 360Learning - Guide technique – JWT SSO
- 360Learning - Guide technique – SSO SAML
- 360Learning - Guide technique – SSO OIDC

2. API

OBJECTIFS

L'API 360Learning prend en charge la synchronisation bidirectionnelle d'un annuaire d'utilisateurs avec celui des utilisateurs 360Learning. Vous pouvez facilement ajouter ou supprimer des utilisateurs, ainsi que définir leur nom, leur mot de passe et les caractéristiques principales de leur profil. Vous pouvez ajouter des utilisateurs à des groupes, par exemple, pour tenir les groupes 360Learning informés des changements au sein de votre organisation.

L'API vous permet également d'exporter des statistiques d'apprentissage relatives à un programme.

Plus généralement, l'API désigne les interfaces logicielles de la plateforme 360Learning qui permettent l'échange de données entre la plateforme et votre système d'information, y compris tout logiciel édité par un tiers pour lequel vous disposez d'un droit d'utilisation.

DOCUMENTATION

La documentation de l'API est disponible en ligne à l'adressehttps://api.360learning.com/
Un guide technique est également disponible pour vous aider à intégrer :

- 360Learning - Guide technique – API

Certaines limitations sur l'utilisation de l'API à connaître sont indiquées dans cette pagehttps://support.360learning.com/hc/en-us/articles/210620943-Guide-technique-API,

Si vous devez exécuter un nombre plus élevé de requêtes, nous vous suggérons de rythmer les appels par lots ou de définir une minuterie sur les scripts.

CONDITIONS D'UTILISATION

L'accès et l'utilisation des API de la plateforme 360Learning sont soumis à l'acceptation et au respect des présentes Conditions d'Utilisation, qui définissent les conditions dans lesquelles 360Learning met à disposition l'API, ainsi que les droits et obligations liés à l'utilisation de l'API.
Les API font partie intégrante des Services et ne sont donc ouvertes qu'à :

- Aux clients d'une entité du groupe 360Learning disposant d'un contrat en vigueur régissant les conditions contractuelles relatives aux Services de la plateforme pour une durée minimale de douze mois et dans le respect de la politique de disponibilité des API déterminée par 360Learning ;
- Aux partenaires ayant conclu un contrat avec 360Learning SA, en tant que titulaire des droits sur la plateforme, définissant les modalités d'accès et d'utilisation des API.

Les Conditions d'utilisation peuvent être mises à jour périodiquement. Les conditions applicables sont celles disponibles en ligne dans la Documentation à la date d'utilisation de l'API.

CONDITIONS GÉNÉRALES D'ACCÈS

Vous accédez et utilisez l'API selon les termes du contrat signé avec 360Learning.
Les conditions et limites d'accès sont définies dans le Guide technique de l'API.
En tant que responsable du traitement des données, il est de votre responsabilité d'utiliser l'API conformément aux règles régissant la protection des données personnelles. Vous garantissez à 360Learning que vous utiliserez les API conformément aux droits des détenteurs des systèmes avec lesquels vous les implémentez.
Dans le cas où un tiers accède et utilise l'API, cette utilisation est réalisée sous votre responsabilité au bénéfice exclusif de vos utilisateurs couverts par le contrat conclu entre vous et 360Learning (affiliés, prestataires de votre système d'information, éditeurs).

Dans ce contexte, l'API est mise à votre disposition uniquement pour un usage technique et interne. Il est interdit de :

- détourner l'utilisation de l'API à des fins commerciales ;
- commettre tout acte de contrefaçon, notamment donner accès, en tout ou partie, à l'API à un tiers à des fins de décompilation ou d'étude de la plateforme ou à des fins de concurrence déloyale ;
- perturber le bon fonctionnement de l'API et, plus généralement, de la plateforme et des Services ;

Vous devez vous assurer que le matériel informatique utilisé pour accéder à l'API est conforme aux normes de sécurité les plus récentes. Vous respectez les procédures et règles de sécurité prescrites par 360Learning.
360Learning se réserve le droit de suspendre l'accès à l'API en cas de suspicion légitime de non-respect des conditions d'utilisation de l'API.

PROPRIÉTÉ DE L'API ET CONTINUITÉ

360Learning détient les droits sur l'API et agit en tant que gestionnaire de l'API.
360Learning peut déprécier, modifier ou limiter l'accès aux API. Dans ce cas, elle en informera ses clients sans délai.

360Learning ne saurait être tenue responsable des conséquences de ces modifications, ne s'engageant pas à assurer la continuité des API. En cas de dépréciation, de modification ou de limitation d'accès entraînant une détérioration significative des Services impactant les conditions déterminantes de la

souscription du contrat, le client peut résilier le Contrat moyennant un préavis écrit de trente (30) jours. Sauf opposition légitime de 360Learning, la résiliation prendra effet à la date d'expiration du préavis notifié par lettre recommandée expliquant et démontrant la détérioration significative des Services et le lien direct avec les conditions déterminantes de la contractualisation.

Sous-traitants qualifiés (*pour votre information*) – Utilisation de la plateforme

Nom légal du sous-traitant	Emplacement où sont hébergées les données client	Description des services fournis	Le cas échéant : Mécanisme de transfert en place pour garantir un niveau de protection adéquat des données personnelles transférées vers un pays tiers	Données personnelles traitées
Microsoft	France États-Unis pour les clients américains*	Hébergement de l'infrastructure de 360Learning Services d'IA générative	N / A	Nom de famille, prénom, e-mail, emploi, photo, connexion, statistiques d'utilisation et de manière générale, toutes les données traitées dans le cadre des services.
Scaleway	France	Environnement de test de stockage, pour les clients qui l'ont demandé pour leurs propres besoins	N / A	Nom, Prénom, E-mail, Emploi, Photo, Connexion, Statistiques d'utilisation et en général toutes les données traitées dans le cadre des tests
Amazon SES	UE (Irlande) États-Unis pour les clients américains*	Envoi de courriers de notification	N / A	Courriel, contenu du courriel et inscription au courriel
Amplitude (non utilisé pour les clients allemands)**	NOUS	Statistiques d'utilisation pour les rapports	-DPA signé avec clauses contractuelles types (CCT) -Certifié conforme au cadre de confidentialité des données UE-États-Unis	IDENTIFIANT (pseudonymisation)
Pendo	UE	Notifications de la plateforme, guides et autres communications intégrées à l'application.	N / A	ID (pseudonymisation)

Datadog	UE	Observabilité	N / A	ID (pseudonymisation)
Snowflake Computing Pays-Bas B.V.	UE États-Unis pour les clients américains*	Statistiques d'utilisation pour le reporting, Fonctionnalités de traitement des données du navire (par exemple : recherche de plate-forme)	N / A	Nom, Prénom, Email (*pour les rendre disponibles dans la recherche-Non utilisé pour les statistiques*) - Pour les statistiques : ID (pseudonymisation)
Elastic Search App	UE États-Unis pour les clients américains*	Moteur de recherche pour alimenter la recherche sur la plateforme ; analyse de l'utilisation pour les recommandations	N / A	Nom, Prénom, Email
Workato	UE pour les clients EMEA - États-Unis pour les clients américains	Fournisseur iPaaS pour les automatisations et les intégrations tierces	N / A	Uniquement pour les connecteurs Workato :données personnelles téléchargées sur le service, qui peuvent inclure, sans s'y limiter :Nom, Prénom, Email.
Les sous-traitants autorisés suivants ne peuvent avoir accès qu'à un nombre limité d'utilisateurs autorisés ayant un rôle spécifique : Auteur, administrateur, propriétaire				
Zendesk	UE pour les clients EMEA*** - États-Unis pour les clients américains***	Gestion des demandes d'assistance client	-Accord de partenariat numérique signé avec clauses contractuelles types (CCT) -Certifié conforme au cadre de confidentialité des données UE-États-Unis	Nom, Prénom, Email, Photo (si ajoutée)

* Pour les clients américains ayant signé un contrat avec 360Learning INC et ayant spécifiquement fait la demande de voir leurs données stockées dans des data-centers américains.
** Pour les clients allemands ayant signé un contrat avec 360Learning GmbH.
***Dans des circonstances exceptionnelles et pour garantir un support efficace en cas de réception d'un nombre élevé de demandes, les opérateurs américains peuvent servir les clients de l'UE et les clients américains peuvent être servis par les opérateurs de l'UE.

Afin de fournir le meilleur service à nos clients, cette liste peut changer.

Pour plus d'informations sur le traitement des données personnelles, nous vous invitons à consulter notre politique de confidentialité accessible depuis le lien suivant : https://360learning.com/privacy-policy

Informations légales

Cookies et statistiques

L'accès à la plateforme 360Learning nécessite l'utilisation de cookies. Ces cookies sont essentiels et/ou fonctionnels, c'est-à-dire nécessaires à la fourniture des services. Leur traitement est basé sur l'intérêt légitime, conformément au RGPD, et ne nécessite pas de consentement spécifique.

Ci-dessous, la description de ces cookies fonctionnels :

Nom du cookie	Utilisation du cookie	Données personnelles traitées par le cookie	Durée de conservation des cookies	Finalité de l'utilisation de ce cookie	Pays du service lié au cookie
globalization_lang	Langue de la session	N/A	Session	Fonctionnalité de l'application	FR / US*
jwt	Première authentification et inscription SSO	N/A	Session	Identification	FR / US*
platformRedirectionPath	Redirection d'URL après authentification	N/A	Session	Confort d'utilisation	FR / US*
refreshToken	Identifiant pour obtenir un nouveau jeton si le jeton d'origine expire (15 min)	N/A	30 jours	Sécurité de la session	FR / US*
rememberMe	Durée avant expiration du token	N/A	30 jours	Sécurité de la session	FR / US*
resetToken	Token utilisé pour définir un mot de passe	N/A	24 heures	Sécurité de la session	FR / US*
route	Accès direct aux fonctionnalités depuis l'authentification	N/A	Session	Sécurité de la session	FR / US*
signToken	Jeton pour créer ou activer un utilisateur	N/A	30 jours	Sécurité de la session	FR / US*
stayInBrowser	Préférence/Web sur appareil mobile	N/A	Session	Confort d'utilisation	FR / US*
singleUseTokenError	Afficher un message d'erreur spécifique	N/A	Session	Debug	FR / US*
subtitle_display	Préférence d'affichage ou non des sous-titres	N/A	Session	Confort d'utilisation	FR / US*
tempToken	Jeton temporaire pour l'authentification SSO (Safari)	N/A	Session	Sécurité de la session	FR / US*
token	Jeton JWT pour l'authentification HTTP uniquement	N/A	15 minutes	Sécurité de la session	FR / US*
tvXXXX	Nombre d'éléments par page à afficher en mode tableau	N/A	Session	Fonctionnalité de l'application	FR / US*
unauthorize DLP	Afficher un message d'erreur	N/A	Session	Debug	FR / US*

user_lang	langue de l'interface	N/A	12 mois	Confort d'utilisation	FR / US*
presetTimeRange	Type de créneau horaire pour le filtre de date	N/A		Fonctionnalité de l'application	FR / US*
Amplitude Tracker	Suivi de l'utilisation des services Amplitude	ID (pseudonymisé)	12 mois	Statistiques	USA**
Amp_XXX	Tracker Amplitude		12 mois	Statistiques	USA**
_dd_s	Journalisation des erreurs du front-end Datadog	ID pseudonymisée	12 mois	Debug	FR / US*

* Les cookies restent dans le pays d'utilisation de la plateforme. France (FR) pour l'utilisation plateforme EMEA, USA pour l'utilisation de la plateforme NA.
**Pays partiellement adapté. Amplitude est membre du Cadre de protection des données UE-États-Unis. Des mesures supplémentaires de protection des données personnelles ont été mises en place, telles que la souscription à un accord de protection des données conforme et les clauses contractuelles types de la Commission européenne.

.

En tant que responsable du traitement des données, 360Learning collecte et traite les données personnelles de ses clients et de leurs employés à des fins de gestion commerciale et administrative. Des statistiques d'utilisation pseudonymisées sont également collectées pour permettre l'analyse et l'amélioration de nos services. 360Learning peut être amené, à des fins exclusives d'administration et de gestion, à partager ces données personnelles avec ses prestataires de services et/ou ses filiales.

360Learning prend toutes les précautions nécessaires lors de la collecte et du traitement des données personnelles des clients afin de se conformer à la législation applicable. Pour toute demande d'accès, d'opposition, de rectification, de portabilité, de limitation ou de gestion des données en cas de décès : les clients peuvent envoyer un e-mail à l'adresse suivante :data-protection@360Learning.com.

Les données personnelles du client sont conservées pendant une durée conforme aux dispositions légales et proportionnées aux finalités pour lesquelles elles ont été enregistrées. Lorsque leur conservation n'est plus justifiée par des exigences légales ou commerciales, par la gestion du compte du client, ou si le client fait usage de l'un de ses droits, tel qu'un droit d'opposition ou d'effacement, nous supprimons les données de manière sécurisée.

Politique de modération

Les présentes règles d'utilisation ont pour objet de définir les principes et modalités de modération des contenus publiés sur la plateforme 360Learning par le Client et ses Bénéficiaires.

Elles visent à garantir un environnement conforme aux exigences légales du règlement européen sur les services numériques du 19 octobre 2022 (« DSA »), au titre duquel 360Learning est qualifié de « prestataire

de services d'hébergement ». Les présentes dispositions ne dispensent pas les clients de leur obligation d'insérer leur propre charte de modération sur la plateforme, destinée à leurs utilisateurs.

Principes généraux applicables à l'utilisation de la plateforme 360Learning :
Lors de l'utilisation de la plateforme 360Learning, les Clients et Bénéficiaires doivent respecter les principes généraux suivants :

- Conformité à la loi : tout contenu publié sur la plateforme 360Learning doit être conforme à la réglementation applicable, notamment aux lois relatives à la diffamation, au harcèlement et au droit d'auteur ;
- Politesse et respect d'autrui : Les utilisateurs de la plateforme doivent se traiter mutuellement avec respect, même en cas de désaccord. Ils doivent s'abstenir de tout propos haineux, discriminatoire ou offensant.
- Les commentaires sur le forum doivent porter uniquement sur des échanges concernant des contenus dans le cadre de l'Apprentissage Collaboratif ;
- Confidentialité et vie privée : Le partage des informations personnelles d'autres utilisateurs sans leur consentement est strictement interdit ;
- Authenticité et propriété intellectuelle : Les utilisateurs doivent s'assurer que le contenu qu'ils publient est authentique et qu'ils détiennent les droits de propriété intellectuelle nécessaires ;
- Véracité des informations : La diffusion de fausses informations ou de contenus trompeurs est strictement interdite.

Responsabilité des contenus publiés sur la plateforme 360Learning par les Clients et leurs Bénéficiaires :
Conformément au Contrat, les Services proposés par 360Learning ont pour objet de fournir l'accès et l'utilisation d'une plateforme permettant aux Clients et Bénéficiaires de créer une expérience de formation engageante et collaborative à travers la création et la mise à jour de contenus de formation à des fins pédagogiques.
Les clients, responsables du contenu publié sur la plateforme, sont tenus de publier leur propre charte de modération. 360Learning, en tant qu'hébergeur, peut suspendre ou supprimer tout contenu considéré comme illicite au regard des lois applicables ou figurant sur la liste suivante :

Catégories de contenu illégal :

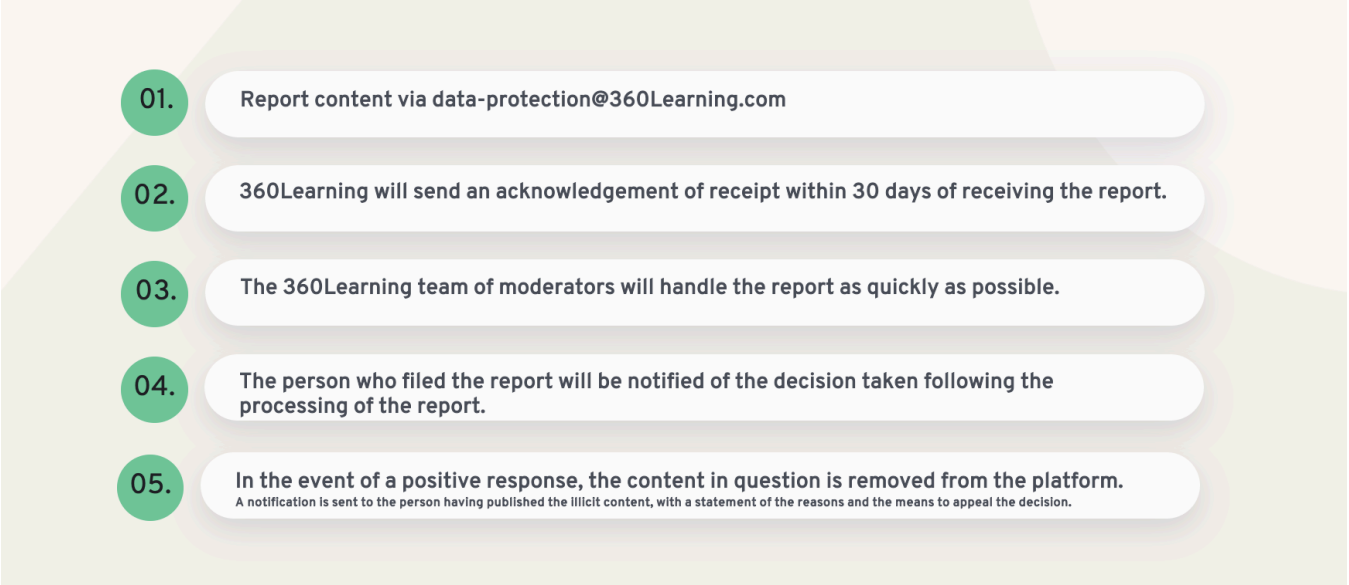
- Contenu illicite : Contenu contraire au droit français et européen, tel que discours de haine, apologie du terrorisme, pornographie enfantine, etc. ;
- Contenu haineux ou discriminatoire : Contenu qui incite à la haine, à la violence ou qui discrimine un individu ou un groupe de personnes en raison de leur origine, de leur religion, de leurs opinions politiques, etc. ;
- Contenu portant atteinte à la vie privée : Contenu qui divulgue des renseignements personnels sans le consentement de la personne concernée ;
- Contenu sexuellement explicite : Contenu pornographique ou sexuellement explicite, y compris la représentation de mineurs ;
- Contenu faux ou trompeur : Contenu qui diffuse de fausses informations ou est susceptible d'induire les utilisateurs en erreur ;

- Contenu plagié : Contenu sur lequel l'utilisateur qui le publie ne possède aucun droit de propriété intellectuelle.

Rapport au client :
Il est rappelé aux clients qu'ils sont responsables du contenu publié sur la plateforme, et qu'il leur appartient de le valider avant qu'il ne soit partagé.

La plateforme permet aux Clients d'intégrer une charte de modération, ainsi qu'une procédure de modération et de signalement des contenus illicites ou contraires à la politique de modération déterminée par le client.
Pour plus de détails sur cette procédure, veuillez lire cet article : Charte de modération
Signalement des commentaires : La plateforme offre également la possibilité de signaler les commentaires illicites ou contraires à la charte de modération définie par le Client, en utilisant le bouton « Signaler » présent sur chaque commentaire. Ce signalement sera traité par le Client conformément à ses propres politiques internes. Pour plus de détails sur cette procédure, veuillez consulter cet article :Rapporter des commentaires

Mécanisme de signalement de contenu illicite à 360Learning, agissant en tant que fournisseur de services d'hébergement :



Tout contenu illicite ou contraire à la politique de modération de 360Learning peut être signalé en envoyant un e-mail à l'adresse suivante : data-protection@360Learning.com
Pour être pris en compte, le rapport doit contenir au moins :

- Les coordonnées de la personne qui fait le signalement ;

- Les coordonnées de l'entité donnant accès à la plateforme (le Client) ;
- Le lien URL et toute autre information sur l'emplacement du contenu ;
- Les raisons pour lesquelles le contenu est considéré comme illicite.

360Learning enverra un accusé de réception à la personne ayant fait le signalement dans les 30 jours suivant la réception du signalement.
Les signalements de contenu adressés à 360Learning seront traités par l'équipe de modérateurs de 360Learning le plus rapidement possible.

La personne qui fait le signalement sera informée de la décision prise suite au traitement du signalement. En cas de réponse positive au signalement, le contenu concerné sera supprimé de la plateforme. Une notification sera également envoyée à l'utilisateur ayant publié le contenu illicite et au client fournissant l'accès à la plateforme, avec un exposé des motifs de la décision et les moyens de recours contre la décision de restriction du contenu après traitement du signalement.
Conformément à ses obligations en vertu de la DSA, 360Learning a désigné data-protection@360Learning comme son point de contact unique pour toutes les communications.