

UPSKILL FROM WITHIN

Documentation technique

Version 6.6 (février 2026)



Chez **360Learning**, nous ne faisons pas de promesses sur les solutions techniques, nous prenons des engagements.

Vos données vous appartiennent. Vos données sont et resteront disponibles pour vous. Pour vous, et vous seul.

360LEARNING EST UN ACTEUR EUROPÉEN DE PREMIER PLAN DES SOLUTIONS CLOUD



En tant qu'acteur de premier plan des solutions Cloud, nous sommes pleinement engagés à fournir à nos clients un haut niveau de sécurité, des SLA et un respect de la vie privée, à la fois dans les engagements contractuels que nous prenons et dans l'infrastructure technique que nous construisons. Nous nous conformons aux exigences légales françaises, qui sont les plus strictes en matière de Données, de Sécurité et de Vie privée.

Benjamin Marchal

CEO, 360Learning

| Pour plus d'informations, n'hésitez pas à nous contacter :

product@360learning.com / www.360learning.com



Sommaire

Vos données vous appartiennent	4
Vraiment	4
Nos droits	4
Confidentialité	4
Pseudonymisation	4
Disponibilité	5
1. Configuration minimale	5
2. Contenus	7
3. Accessibilité	8
4. Développement	10
Sécurité	13
1. Chiffrement	13
2. Sécurité physique	14
3. Sécurité logique	17
4. Politiques internes	21
5. Sécurité de l'application mobile	24
6. Audits indépendants	24
7. Standards	25
Continuité de service	26
1. Politiques internes	26
2. Sauvegardes	26
3. Redondance	27
4. Reprise de service	27
Scalabilité	30
1. Occupation système	30
2. Volume client	33
Intégrations	34
1. SSO	34
2. API	35
Sous-traitants autorisés (pour information) - Utilisation de la plateforme	37
Informations légales	39

Vos données vous appartiennent

| Vraiment

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

À la fin du contrat, le client peut demander à 360Learning de récupérer l'intégralité de son catalogue de formations dans un format standard.

| Nos droits

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

- Questions du client concernant ses données
- Résolution d'incidents
- Demandes du client de modification des données

| Confidentialité

360Learning garantit qu'aucune donnée à caractère personnel à laquelle elle a accès en qualité de sous-traitant pour la fourniture des services contractés n'est vendue, transférée ou divulguée à des tiers à des fins commerciales.

| Pseudonymisation

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

| Disponibilité

1. Configuration minimale

PLATEFORME

Une configuration minimale est requise pour bénéficier pleinement de l'application 360Learning :

- Vérifier les prérequis suivants concernant le poste de travail : résolution d'affichage minimale de 1024x600 pixels et 256 Mo de RAM.
- S'assurer que tous les postes disposent d'un navigateur compatible : Microsoft Edge, Mozilla Firefox, Google Chrome ou Apple Safari, dans une version supportée par l'éditeur.
- Effectuer des tests de bande passante réseau afin de déterminer la bande passante disponible pour les formateurs et les apprenants, et optimiser la configuration réseau selon le type de formats pédagogiques proposés, pour une diffusion et une consommation optimales des contenus de formation.

Bande passante minimale requise pour la connexion Internet : 512 kbps par poste de travail pour l'ensemble des usages, y compris le streaming vidéo (dans les conditions précisées au paragraphe « Vidéo » ci-dessous) et hors modules SCORM.

- Authentifier les serveurs de messagerie afin que les e-mails envoyés par la plateforme ne soient pas bloqués par la DSI du client. L'adresse e-mail no-reply@360learning.com doit être ajoutée à la liste blanche dans le champ « from » (et non dans le champ d'adresse du serveur SMTP) au sein des paramètres du client de messagerie, du serveur de messagerie et du logiciel anti-spam. Si vous personnalisez par la suite l'adresse d'envoi des notifications de la plateforme, vous devez également l'ajouter à la liste blanche dans ces emplacements. Si vous ne pouvez pas filtrer sur le champ « from », vous pouvez ajouter à la liste blanche les adresses IP suivantes :

IP de l'environnement de production :

- 52.252.128.38
- 52.252.135.139
- 20.74.1.94
- 20.88.12.20
- 135.119.57.91
- 20.111.17.162
- 20.74.25.229
- 20.74.30.34
- 20.74.30.77
- 4.178.179.114
- 4.178.179.34
- 4.211.206.17
- 4.233.88.150
- 51.138.202.254
- 52.228.185.142
- 54.240.50.243
- 54.240.50.244

IP de l'environnement de pré-production :

- 20.40.143.206

- 20.74.25.131
 - 20.188.57.169
 - 4.251.105.167
 - 40.78.168.160
 - 40.78.176.167
 - 52.143.157.167
- Ajouter à la liste blanche *.360learning.com ou le nom de domaine personnalisé pour garantir l'accès des utilisateurs à la plateforme.
 - Ajouter à la liste blanche les domaines ci-dessous pour accéder aux banques d'images Unsplash et Pixabay <https://unsplash.com/>
<https://pixabay.com/>
 - Optionnel : si vous prévoyez d'utiliser des modules SCORM, assurez-vous que les pop-ups sont autorisées.
 - Optionnel : ajouter à la liste blanche api.amplitude.com et cdn.amplitude.com afin que la R&D de 360Learning dispose des outils analytiques nécessaires pour détecter les erreurs, corriger les bugs au plus vite et améliorer en continu l'expérience utilisateur.

Pour vous aider à vérifier l'ensemble des 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 supportées :

- iOS 16 et supérieur
- Android 8 et supérieur

Sur les terminaux mobiles, nous ne fournissons un support que pour nos applications mobiles natives. Bien que notre plateforme soit responsive, nous ne supportons pas les navigateurs web mobiles. Toute publication ou mise à jour d'application personnalisée est soumise aux délais propres aux marketplaces concernées (Google Play Store, Apple App Store, etc.), qui restent hors de notre contrôle.

Nos applications mobiles couvrent principalement le cas d'usage Apprenant (Learner), mais prennent également en charge certains cas d'usage Coach et Manager.

Elles supportent en outre une large palette de contenus de formation et de formats de fichiers, notamment :

- Aide-mémoires 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)
- Contenus partageables depuis le web (lien direct, code d'intégration ou code iframe ; nécessite une connexion Internet)

VIDÉO

360Learning prend en charge l'import de vidéos HD et crée automatiquement des versions SD en moyenne 5 fois plus légères que les fichiers d'origine. Un sélecteur HD/SD est disponible en bas à droite du lecteur afin que les utilisateurs puissent choisir la qualité de streaming souhaitée. À noter que le lecteur adapte automatiquement la qualité vidéo à la bande passante disponible, et que les utilisateurs cliquant sur HD consomment davantage de bande passante.

Pour maîtriser la consommation de bande passante, veillez à ce que le bitrate de vos fichiers vidéo soit inférieur ou égal au débit attendu sur le réseau cible. Par exemple, si la consommation de bande passante souhaitée en SD et HD doit rester inférieure à 512 kbps, importez des fichiers source dont le bitrate est inférieur à 512 kbps.

2. Contenus

La plateforme 360Learning permet la création d'aide-mémoires et de plusieurs types de questions, notamment vrai/faux, choix multiples, remise en ordre, association, zones sensibles, questions ouvertes, etc.

Vous pouvez également importer divers types de documents :

- Audio : .mp3, .m4a, .wav, .ogg, .aac, .opus
- AutoCAD : .dwg
- Archives : .zip, .rar, .7z, .rbz, .a
- CAO : .stl
- Calendrier : .ics
- Code-barres : .btw
- Ebook : .azw3, .epub
- Excel : .xlsx, .xls, .xlsm, .ods, .csv, numbers, .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
- Mail : .msg, .eml
- Mathematica : .mm
- Rapport Microsoft Power BI : .pbix

- Mindmap : .xmind, .mvdX
- Modélisation : .rfa, .ifc
- Musique : .enc
- Rapport réseau : .pkt
- One Note : .one
- PDF : .pdf, .xps
- Projet : .gan
- Publisher : .pub
- Question : .quiz
- Tableau : .twb
- Texte : .log
- Texte brut : .txt, .md
- Diaporama : .pptx, .ppt, .ppsx, .odp ; .pptm, .ppsm, .pps, gslides, flipchart, .ppta
- Vault : .dvs
- Vidéo : .wmv, .vob, .mts.mpg, .mpeg, .mkv, .m2ts, .flv, .3gp, .mp4, .webm, .mov, .m4v, .3gpp, .m2t, .avi
- Word : .docx, .doc, .odt, .pages, .rtf, .story, .dotx, .dot, .wps, .sdoc
- Modules SCORM, version 1.2 ou 2004

Les contenus partageables depuis le web (lien direct, code d'intégration ou code iframe) peuvent également être importés, y compris les contenus issus de services tels que YouTube, Slideshare ou Prezi.

3. Accessibilité

360Learning applique les bonnes pratiques de conception centrée sur l'expérience utilisateur (UX). Nos équipes Produit et Design suivent en continu les dernières tendances UX/UI. Nous optimisons l'ergonomie de notre plateforme grâce à des améliorations continues fondées sur les données et les retours utilisateurs.

Chez 360Learning, le design est autant une question de comportement et d'émotion que d'utilité et de praticité. C'est pourquoi l'ergonomie et le design constituent l'un des principaux piliers du LMS, de l'outil-auteur et des fonctionnalités sociales et collaboratives de 360Learning.

360Learning s'inspire des standards et recommandations du W3C (World Wide Web Consortium), le consortium chargé de promouvoir la compatibilité des technologies du Web, ainsi que 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 ceux des collectivités territoriales et des établissements publics qui en dépendent, pour les trois canaux que sont l'internet, la télévision et la téléphonie.

À la suite d'un audit mené par notre partenaire accessibilité Level Access en janvier 2025, nous sommes partiellement conformes au niveau AA des WCAG et nous poursuivons nos efforts en matière d'accessibilité.

Voici les éléments de conformité présents sur la plateforme 360Learning :

LISIBILITÉ

- La police utilisée est Plus Jakarta Sans. Une police claire et simple, qui améliore la lisibilité.
- L'usage des majuscules est strictement limité.
- Sous-titres générés automatiquement disponibles sur les vidéos de cours (la consommation vidéo standard est plafonnée à 2,5 heures/utilisateur/an).
- 360Learning privilégie des combinaisons de couleurs très contrastées qui favorisent une lisibilité optimale. Par exemple : blanc/noir – bleu foncé/blanc. Nous veillons à ce que la combinaison entre la couleur du texte et celle du fond ne descende pas sous le ratio recommandé de 4,5:1 pour le texte standard (< 19 px) et de 3:1 pour le texte de plus grande taille (=> 19 px).

BARRE DE NAVIGATION

Nous fournissons des barres de navigation standard, toujours positionnées au même endroit, ainsi qu'un outil de recherche et des liens d'évitement.

ZONAGE & LISIBILITÉ COGNITIVE

La navigation sur 360Learning est semi-guidée.

Chaque zone est nettement séparée et correspond à une activité.

La structure de chaque cours est identique, ce qui permet à l'utilisateur de simplifier et de mémoriser le parcours de navigation.

ÉLÉMENT D'ORIENTATION UTILISATEUR

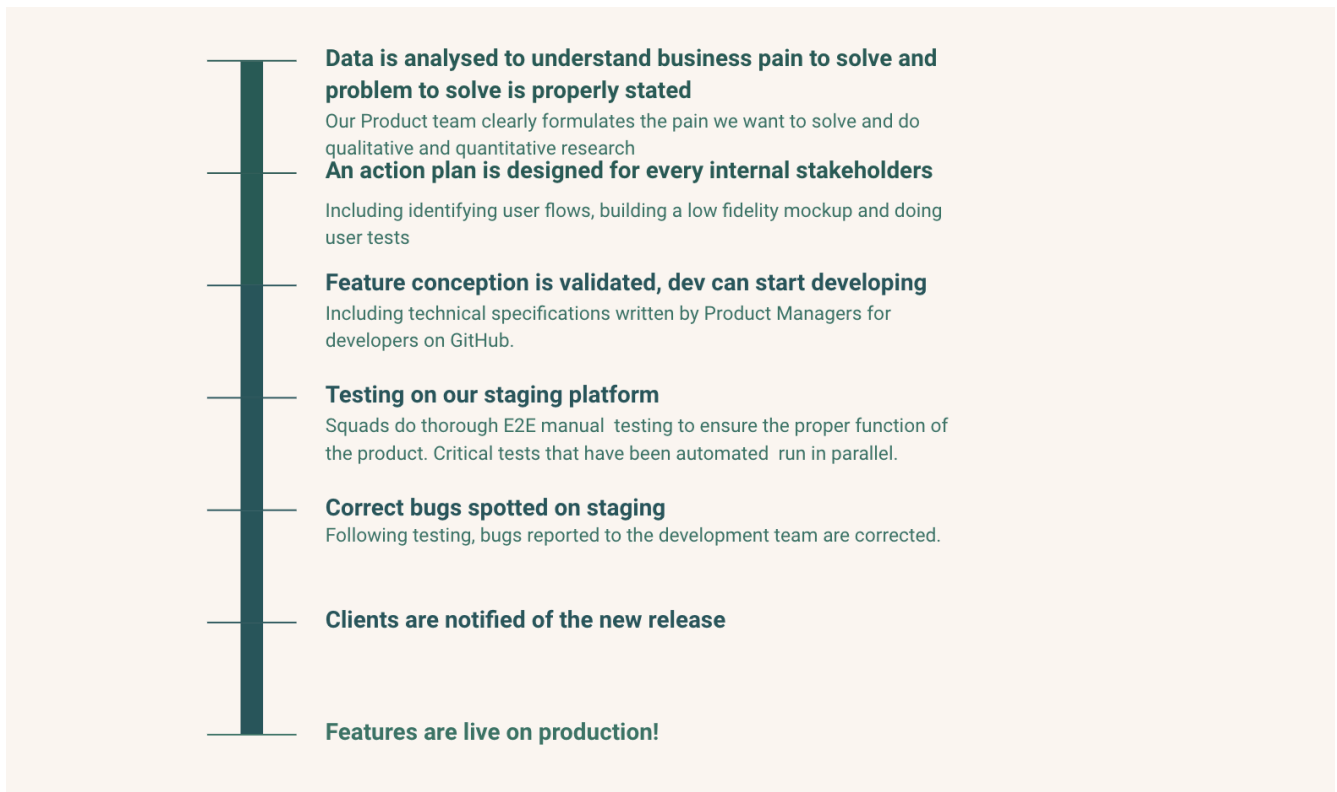
La plateforme permet à l'apprenant d'identifier facilement, à tout moment, la page affichée parmi celles du site. En particulier, l'interface fournit un élément qui aide l'apprenant à déterminer :

- Où il se trouve : le menu correspondant s'affiche en gras et avec une luminosité accrue
- D'où il vient : l'apprenant peut se situer à tout moment dans le programme (fil d'Ariane)
- Où il peut aller ensuite : l'apprenant peut se projeter dans son parcours

4. Développement

NOUVELLES FONCTIONNALITÉS

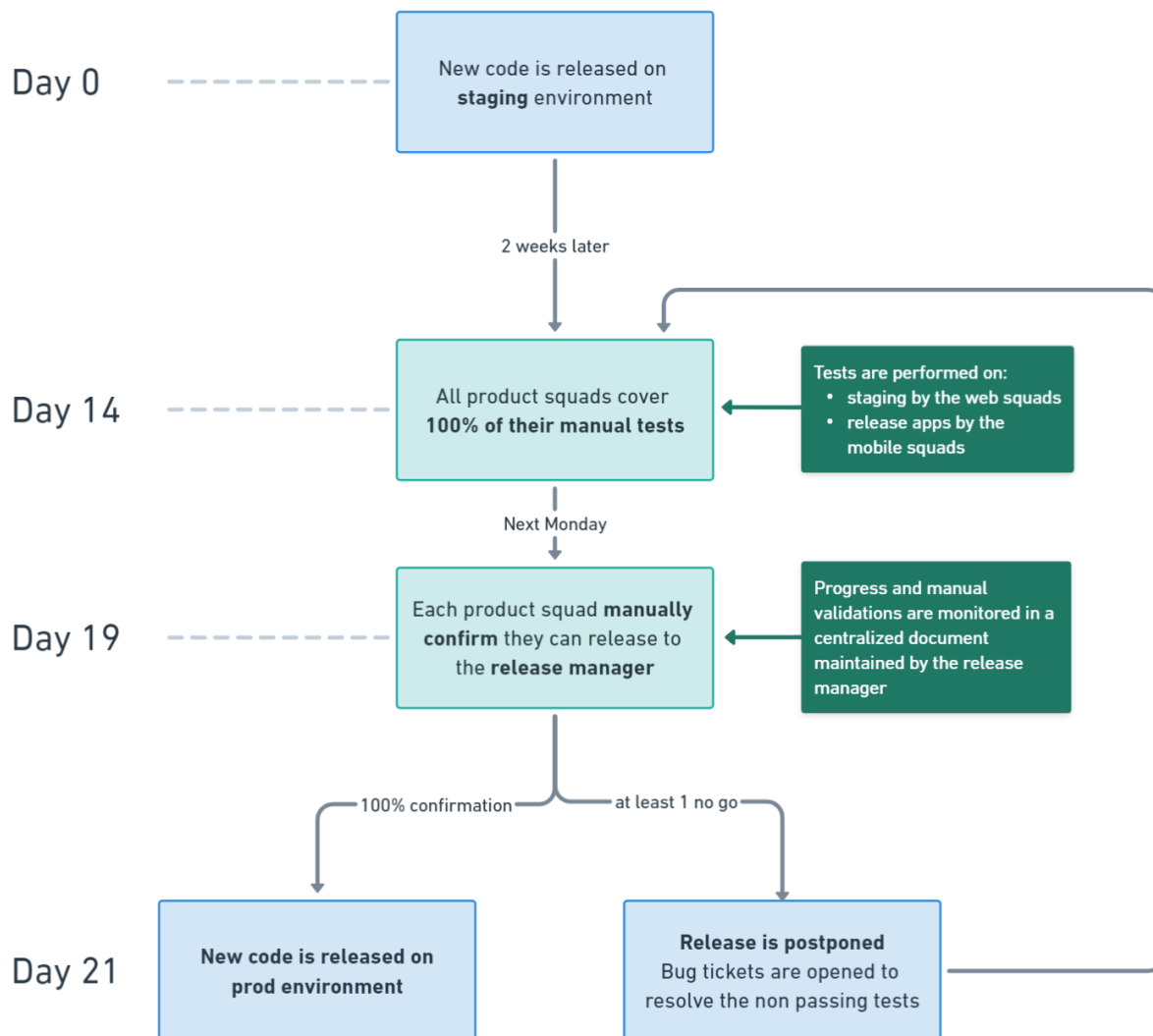
Chaque nouvelle fonctionnalité est développée selon un plan très précis, détaillé ci-dessous.



ASSURANCE QUALITÉ

Chaque fonctionnalité est testée sur un **environnement de staging** avant son déploiement sur l'**environnement de production**, selon le processus détaillé ci-dessous. 🙌

Pour garantir un niveau de qualité conforme à nos exigences lors de la livraison de fonctionnalités, sans casser les autres fonctionnalités de la plateforme, nous exécutons des tests end-to-end manuels à chaque Milestone. Un release manager est désigné et doit s'assurer que ce processus est respecté, principalement en communiquant avec les Tech Leads pendant la MS.



Environnement de staging

Une réplique quasi exacte de notre environnement de production destinée aux tests logiciels. Nous utilisons l’environnement de staging pour tester les builds dans des conditions proches de la production avant le déploiement applicatif.

Environnement de production

L’environnement où la dernière version de notre plateforme est en ligne pour les utilisateurs. C’est l’environnement dans lequel les utilisateurs finaux peuvent voir, expérimenter et interagir avec le produit.

Personnalisation de l’apparence de la plateforme via du CSS personnalisé (option facultative)

360Learning peut décider de proposer, à titre de geste commercial et gracieusement, du CSS personnalisé à un client de 360Learning qui en fait la demande. Cette option ne peut être activée que par

l'Account Manager et sous certaines conditions. Les recommandations générales relatives au CSS personnalisé sont décrites dans cet article de la base de connaissances 360Learning :

<https://support.360learning.com/hc/en-us/articles/4956106195732-Customize-platform-appearance-with-custom-CSS>

Le client est responsable et juridiquement engagé pour l'ensemble des modifications apportées à sa plateforme via du CSS personnalisé. 360Learning ne procède pas à la mise en place, à la maintenance, à la garantie d'interopérabilité ni au support du code personnalisé. À titre d'exemple, si un client estime que le CSS personnalisé est adapté à ses besoins, les Owners de la plateforme doivent être prêts à :

- Tester le code personnalisé à chaque release, qui survient [toutes les 3 semaines](#).
- Gérer, diagnostiquer et supporter tout incident lié au code personnalisé.

360Learning : (i) peut désactiver à tout moment le CSS personnalisé du client, en particulier si 360Learning identifie des problèmes de sécurité ou de performance ; et (iii) ne fournit aucune garantie expresse ou implicite, de quelque nature que ce soit, sur le CSS personnalisé.

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

| Sécurité

1. Chiffrement

Par défaut, l'accès à l'application est systématiquement forcé en HTTPS TLS 1.2 minimum, avec un ensemble compatible de suites de chiffrement robustes.

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

#TLS 1.2

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048)

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)

TLS_ECDHE_RSA_WITH_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 assurer une compatibilité maximale avec les navigateurs récents tout en garantissant un niveau de sécurité maximal. La compatibilité ne devrait pas poser de problème, sauf si vous utilisez un navigateur ou des bibliothèques client HTTP anciens.

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 sa première connexion.
- Par un administrateur lors de la création du compte.
- Via le mécanisme SSO, auquel cas 360Learning stocke en base une chaîne aléatoire de 32 caractères en lieu et place du mot de passe.

Une fois ce mot de passe défini, il est impossible pour un tiers d'en prendre connaissance par une requête sur notre base, dans la mesure où tous les mots de passe sont hachés de manière irréversible avec BCRYPT 10 rounds. En cas de détection d'une attaque, nous notifierions tous les clients concernés dans les meilleurs délais.

CONTRÔLE D'ACCÈS PAR ADRESSE IP

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

2. Sécurité physique

DATA CENTERS HAUTEMENT SÉCURISÉS

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

CARACTÉRISTIQUES DES DATA CENTERS – Microsoft Azure

Sécurité et incendie

- Contrôle d'accès autonome par badge sans contact RFID, et biométrie par reconnaissance du réseau veineux du doigt
- Sas d'entrée à double porte blindée conforme aux normes anti-intrusion EN1627
- Réseaux de caméras numériques en intérieur et en extérieur
- Dispositifs anti-intrusion sur tous les points d'accès (APSAD R81) et APSAD R81 (détection d'intrusion)
- Responsable sécurité incendie qualifié SSIAP 2, présent 24/7
- Systèmes de détection multi-points VESDA LASER
- Systèmes d'extinction par brouillard d'eau SEMCO, conformes aux normes APSAD R1/D2 et NFPA 750
- Moyens complémentaires d'extinction par RIA et extincteurs portables CO2 conformes à la norme APSAD R4
- Compartimentage coupe-feu entre chaque salle informatique, capable de résister au feu pendant deux heures

Alimentation électrique	Climatisation
<ul style="list-style-type: none">● Alimentation depuis le réseau EDF via 2 arrivées en T bidirectionnelles de 9 MVA chacune● 7 tableaux généraux basse tension I de 2,5 MVA chacun, équipés d'un basculement automatique vers la redondance par groupe électrogène● 6 groupes électrogènes diesel pour une capacité installée de 11,85 MVA● 48 800 litres de fioul, soit 50 heures d'autonomie à pleine charge● Zone N+1 : 3 chaînes onduleur indépendantes● Zone 2(N+1) : 2 chaînes onduleur indépendantes● Autonomie batterie : 10 minutes en fin de vie des batteries	<ul style="list-style-type: none">● 5 MW de puissance frigorifique en configuration N+1● Réseau d'eau glacée redondant en boucle (circuits de distribution)● Armoires de climatisation de 90 kW● Température maintenue à 20 °C +/- 2 °C en allée froide● Confinement systématique de l'allée froide● Climatisation indépendante pour chaque salle client
Bâtiments	Maintenance et gestion technique des bâtiments
<ul style="list-style-type: none">● Conception et construction spécifiquement dédiées à un usage de data center	<ul style="list-style-type: none">● Maintenance conforme aux normes AFNOR NF EN 13-306 et FD X60-000● Télésurveillance des équipements par les fabricants● Gestion technique des installations par GTC Sima©

CARACTÉRISTIQUES DES DATA CENTERS – AWS

Sécurité et incendie

- L'accès physique aux serveurs informatiques est restreint aux collaborateurs habilités
- Accès contrôlé par authentification multi-facteurs, sites gardés par des agents de sécurité professionnels 24/7
- Les points d'accès physiques aux salles serveurs sont enregistrés par vidéosurveillance (CCTV). Les images sont conservées conformément aux exigences légales et de conformité.
- Salles équipées de systèmes de détection de fumée et de chaleur
- Les audits réalisés par des tiers sur les data centers AWS, tels que documentés dans nos rapports d'audit tiers, attestent qu'AWS a correctement mis en œuvre les mesures de sécurité requises pour l'obtention des certifications de sécurité.

Alimentation électrique

- Les systèmes d'alimentation électrique des data centers AWS sont conçus pour être totalement redondants et maintenables sans impact sur l'exploitation, 24 heures sur 24. AWS s'assure que les data centers sont équipés d'une alimentation de secours afin de garantir le maintien de l'alimentation en cas de défaillance électrique pour les charges critiques et essentielles du site.

Climatisation

- Les data centers AWS utilisent des dispositifs de contrôle climatique permettant de maintenir une température de fonctionnement appropriée pour les serveurs et les autres matériels, afin de prévenir les surchauffes et de réduire le risque d'interruption de service. Du personnel et des systèmes surveillent et contrôlent la température et l'humidité à des niveaux adéquats.

Bâtiments

- AWS conçoit et construit ses propres data centers
- Les data centers AWS sur lesquels nous nous appuyons traitent les données dans des data centers situés dans l'UE.
- Les sites sont distants d'au moins 200 km les uns des autres afin de garantir la redondance et la continuité de service

Maintenance et gestion technique des bâtiments

- Des systèmes électroniques de détection d'intrusion sont installés au niveau de la couche data afin de surveiller, détecter et alerter automatiquement les personnes habilitées en cas d'incident de sécurité. Les points d'entrée et de sortie des salles serveurs sont sécurisés par des dispositifs imposant une authentification multi-facteurs à chaque personne avant toute entrée ou sortie.

3. Sécurité logique

Ceci est un résumé synthétique de nos éléments de sécurité. Pour plus de détails, veuillez consulter notre Plan d'Assurance Sécurité v3.4

PRÉVENTION DES ATTAQUES PAR DÉNI DE SERVICE (DDoS)

Une attaque DDoS vise à rendre votre site indisponible en saturant la bande passante du serveur ou en occupant ses ressources jusqu'à épuisement. Les cas rencontrés sont généralement des attaques de niveau 7 (le plus élevé), reposant 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 son service figurent parmi les priorités majeures de 360Learning. Pour contrer ces attaques, notre hébergeur Microsoft Azure adopte en standard une solution de mitigation reposant sur la technologie VAC. Elle consiste en une combinaison exclusive de techniques qui analysent votre trafic en temps réel et à haute vitesse. Elles détectent et interceptent automatiquement les attaques tout en laissant passer les requêtes légitimes.

DÉTECTION ET PRÉVENTION DES ATTAQUES OWASP

Un Web Application Firewall Next Generation, placé en frontal de nos serveurs, filtre chaque requête afin d'identifier toute menace potentielle. Il embarque les règles classiques de détection OWASP ainsi que des règles métier spécifiques pour alerter et bloquer les tentatives malveillantes.

Les alertes sont envoyées aux équipes DevOps et Sécurité afin de déclencher, le cas échéant, un incident de sécurité.

Toutes les attaques sont journalisées et conservées au moins 6 mois pour permettre la conduite d'audits de sécurité.

ANTIVIRUS

Notre solution de référence 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 de la base de signatures la plus récente pour la détection et la prévention des menaces. Une analyse est réalisée sur l'ensemble des fichiers et archives importés afin de s'assurer qu'aucun exécutable n'est stocké.

En cas de détection d'un virus, l'utilisateur ayant tenté l'import est notifié par le message suivant : « Votre document semble suspect à notre antivirus. Votre fichier n'a pas été importé. » Et le fichier n'est jamais importé.

DÉTECTION ET REMÉDIATION DES MENACES

Nous avons déployé :

- une solution Endpoint Detection and Response (EDR/XDR) CrowdStrike sur chaque serveur, afin d'assurer un haut niveau de protection et la capacité d'identifier toute menace sur notre plateforme (rançongiciels, malwares, rootkits, remote shell, etc.). Chaque agent est connecté à une plateforme centrale, gérée en externe 24/7 par les équipes CrowdStrike, qui escaladent à l'équipe sécurité interne de 360Learning en cas d'urgence.
- un Web Application Firewall Next Generation qui filtre chaque requête à destination de l'ensemble de nos applications et endpoints externes.
- un SIEM qui corrèle les logs de l'ensemble de nos systèmes corporate et plateforme. Il s'accompagne d'un SOC externe 24/7 qui alerte l'équipe sécurité en cas de comportement anormal (non-conformité, attaque, comportement inhabituel tel qu'une authentification réussie depuis une source inconnue).

RÔLES AU SEIN DE L'APPLICATION

La plateforme prend en charge plusieurs rôles et des jeux de permissions granulaires, ce qui nous permet d'appliquer une politique de contrôle d'accès finement paramétrée selon le rôle de chaque utilisateur.

Les rôles déterminent ce que les utilisateurs peuvent voir et faire dans 360Learning. Les rôles principaux sont conçus pour fixer le niveau d'accès des utilisateurs à la gestion des comptes, des contenus de formation et des paramètres de 360Learning (accès admin). Les rôles spécifiques donnent aux utilisateurs accès à des fonctionnalités plus collaboratives de 360Learning.

RÔLES PRINCIPAUX

Apprenant

Les Apprenants ont accès à la page d'accueil de leurs groupes, peuvent suivre les contenus de formation partagés par les Auteurs, Coachs et Admins, et utiliser les fonctionnalités sociales de la plateforme.

Les Apprenants ne disposent d'aucun accès admin.

Les droits de l'Apprenant incluent :

- Accès aux contenus de formation
- Possibilité de poster des messages dans les groupes et les forums des contenus de formation
- Accès à ses statistiques de formation personnelles

Auteur

Les Auteurs peuvent créer des contenus de formation et les partager dans la bibliothèque de leur groupe.

Les droits de l'Auteur incluent :

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

Coach

Les Coachs peuvent consulter et exporter les statistiques de leur groupe et partager des contenus de formation avec leur groupe.

Les droits du Coach incluent :

- Possibilité de suivre toute formation de la bibliothèque de leur groupe
- Possibilité de créer des sessions à partir des modèles de programmes de la bibliothèque du groupe
- Accès aux statistiques de formation du groupe depuis le menu Dashboard
- Possibilité d'ajouter le groupe à une nouvelle session
- Possibilité d'envoyer des relances

Administrateur d'utilisateurs

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

Les droits de l'Administrateur d'utilisateurs incluent :

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

Administrateur de groupe

Les Administrateurs disposent d'un accès admin complet à leurs groupes. Ils ont également l'ensemble des permissions des Auteurs, Coachs et Administrateurs d'utilisateurs.

Les droits de l'Administrateur incluent :

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

Administrateur de plateforme

Les Administrateurs de plateforme disposent d'un accès admin complet à tous les groupes et d'un accès admin complet à la plateforme, incluant notamment :

- Possibilité de paramétrer le Public Channel (s'ils sont désignés Admin du groupe transverse de la plateforme)
- Accès aux Paramètres avancés de la plateforme (s'ils sont désignés Admin du groupe transverse)
- Accès à la création de badges (s'ils sont désignés Admin du groupe transverse)

Owner

Chaque plateforme dispose d'un unique Owner. Il bénéficie du même niveau de permissions que les Administrateurs de plateforme et est le seul à pouvoir accéder au menu de facturation.

Les droits de l'Owner incluent :

- L'ensemble des permissions de l'Administrateur de plateforme
- Accès aux informations de facturation
- Téléchargement de 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 auteur principal ; ce rôle peut être transféré, et les permissions sont transférées lorsque l'auteur principal est supprimé de la plateforme.

Les droits de l'Auteur principal incluent :

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

Instructeur

Les Instructeurs sont en charge des sessions de programmes et de parcours.

Les droits de l'Instructeur incluent :

- Accès aux statistiques de leurs sessions de parcours et de programmes.
- Réception des notifications relatives au programme (informations de connexion, commentaires, posts, programme terminé)
- Correction des questions ouvertes
- Correction des étapes d'évaluation
- Gestion des participants à la session (ajout/retrait de participants)
- Possibilité d'envoyer des relances depuis les statistiques de la session

Manager

Les Managers peuvent accéder aux statistiques d'un utilisateur (y compris sur des cours ou sessions auxquels ils n'ont pas eux-mêmes accès).

Les Managers peuvent :

- Accéder aux statistiques de leurs collaborateurs depuis le menu Dashboard
- Recevoir un e-mail hebdomadaire présentant la progression de leurs collaborateurs (option désactivable dans leurs paramètres)
- Corriger les étapes d'évaluation

Co-auteur (cours ou parcours)

Les co-auteurs de cours et de parcours disposent des mêmes permissions qu'un auteur principal, mais leurs permissions ne sont pas transférées lors de leur suppression de la plateforme.

Les Co-auteurs peuvent :

- Modifier des cours et des parcours

Reviewer

Les Reviewers peuvent relire des cours et publier des commentaires internes dans le forum de ces cours. Ce rôle n'est disponible qu'avec la solution Champion.

Les Reviewers peuvent :

- Publier des commentaires internes dans un cours

PARE-FEU ET FILTRAGE DE PORTS

Les pare-feux des serveurs de 360Learning fournissent un niveau de sécurité supplémentaire en matière de contrôle des flux. Tous les ports qui ne sont pas nécessaires au fonctionnement et à l'administration de la plateforme sont fermés.

Nous utilisons un outil de Cloud Security Posture Management qui alerte en cas d'ouverture de port non conforme à notre politique de sécurité.

4. Politiques internes

POLITIQUE DE MOTS DE PASSE

1. Présentation

L'ensemble des collaborateurs et personnels ayant accès aux systèmes informatiques de l'organisation doivent respecter notre charte informatique ainsi que les politiques de mots de passe définies ci-dessous, afin de protéger la sécurité du réseau, l'intégrité des données et les systèmes informatiques.

2. Objet

Cette politique a pour but de protéger les ressources de l'organisation sur le réseau en imposant des mots de passe robustes ainsi que la protection de ces mots de passe, et en établissant un délai minimum entre les changements de mot de passe.

3. Périmètre

Cette politique s'applique à toute personne disposant d'un compte informatique, sous quelque forme que ce soit, nécessitant un mot de passe sur le réseau de l'organisation, y compris, sans s'y limiter, les comptes de domaine et les comptes de messagerie.

4. Protection des mots de passe

- Ne jamais noter ses mots de passe
- Ne jamais transmettre un mot de passe par e-mail
- Ne jamais inclure un mot de passe dans un document stocké non chiffré
- Ne jamais communiquer son mot de passe à qui que ce soit
- Ne jamais divulguer son mot de passe par téléphone
- Ne jamais donner d'indication sur le format de son mot de passe
- Ne jamais divulguer ni laisser deviner son mot de passe dans un formulaire en ligne
- Ne jamais utiliser la fonctionnalité « Se souvenir du mot de passe » des programmes applicatifs (client de messagerie ou tout autre programme)
- Ne jamais utiliser son mot de passe d'entreprise ou de réseau sur un compte en ligne dont la connexion n'est pas sécurisée par https:// (au lieu de http://)
- Toujours utiliser notre gestionnaire de mots de passe officiel
- Signaler toute suspicion de compromission de son mot de passe au responsable sécurité informatique
- Si quelqu'un demande votre mot de passe, le rediriger vers le responsable sécurité informatique
- Veiller à ne pas laisser quelqu'un voir la saisie de son mot de passe
- Utiliser le MFA chaque fois que possible

5. Application

La sécurité des mots de passe étant essentielle à la sécurité de l'organisation et de chacun, les collaborateurs qui ne respectent pas cette politique peuvent faire l'objet de mesures disciplinaires pouvant aller jusqu'au licenciement.

Pour assurer le niveau de sensibilisation de nos collaborateurs, nous menons régulièrement des campagnes de faux phishing, des formations et des quiz.

6. Autres considérations

Des économiseurs d'écran protégés par mot de passe doivent être activés et verrouiller le poste après 10 minutes d'inactivité de l'utilisateur. Les postes ne doivent jamais rester sans surveillance avec une session ouverte sans économiseur d'écran protégé par mot de passe actif. Les utilisateurs doivent prendre l'habitude de ne pas laisser leur poste déverrouillé.

Les mots de passe administrateur doivent être protégés avec une vigilance particulière. Les comptes administrateur ne doivent disposer que des accès strictement nécessaires à l'exercice de leur fonction. Les comptes administrateur ne doivent jamais être partagés.

7. Utilisation d'un coffre-fort de mots de passe

L'utilisation d'un gestionnaire de mots de passe, en l'occurrence 1Password, facilite l'application des points ci-dessus.

Quels en sont les apports ?

- Il n'y a qu'un seul mot de passe maître à retenir.
- Il permet de partager l'accès à un compte de manière sécurisée sans communiquer le mot de passe.
- Il permet de générer des mots de passe sécurisés.

Comment cela fonctionne-t-il ?

- Chiffrement AES 256 bits avec un nombre d'itérations PBKDF2 régulièrement augmenté
- Toutes les données sensibles sont chiffrées et déchiffrées localement avant la synchronisation avec 1Password. La clé ne quitte jamais l'appareil et n'est jamais partagée avec 1Password. Nos données restent accessibles uniquement à nous.

5. Sécurité de l'application mobile

- Notre application utilise les mêmes serveurs que notre client web et se connecte également via HTTPS avec TLS 1.2 (TLS 1.3), bénéficiant ainsi des mêmes niveaux de sécurité. À ce titre, les logs sont conservés et traités de la même manière, qu'ils soient générés par l'application mobile ou par l'application web.
- De même, si vous imposez l'acceptation d'une politique de confidentialité, les utilisateurs devront y consentir lors de leur première connexion, quel que soit le client utilisé (mobile ou web).
- Les données de géolocalisation sont pseudonymisées dès leur collecte à des fins d'analyse produit, de sorte qu'aucune donnée à caractère personnel 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 via le système d'exploitation.
- Nos applications mobiles font l'objet d'un test d'intrusion une fois par an.

6. Standards

Raison sociale des sous-traitants				
Microsoft Azure	✓	✓	✗	✓
AWS	✓	✓	✗	✓
Scaleway	✓	✓	✗	✓
Amplitude	✓	✓	✗	✓
Pendo Inc.	✗	✓	✗	✗
MongoDB Atlas	✓	✓	✗	✓
Datadog	✓	✓	✗	✓
Zendesk	✓	✓	✗	✓
Stripe (pour le paiement des offres team)	✓	✓	✓	✗

Snowflake Computing Netherlands B.V.	✓	✓	⊘	✓
Elastic App Search	✓	✓	⊘	✓
Workato	✓	✓	⊘	✗

✓ : Oui

✗ : Non

⊘ : N/A

Continuité de service

1. Politiques internes

Nous garantissons à l'ensemble de nos clients un **taux de disponibilité mensuel de 99,8 %**.

Plus d'informations sur notre SLA sont disponibles sur :

- Pour les clients Essential & Advanced : [\[EN\]SLA](#)
- Pour les clients Ultimate : <https://360learning.com/legal/slaenultimate/>

2. Sauvegardes

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

Région	Data Center Azure (localisation)	Zones de disponibilité	Data Center Azure de secours	Disponibilité commerciale
France	France Central (région parisienne)	3	North Europe (Irlande)	Disponible pour tous les clients
États-Unis	Central US (Iowa)	3	East US (Virginie)	Disponible pour les clients américains

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

Les Availability Zones d'Azure sont des emplacements physiquement distincts au sein de chaque région Azure, tolérants aux pannes locales. Ces pannes peuvent aller de défaillances logicielles ou matérielles à des événements tels que séismes, inondations et incendies. Cette tolérance est obtenue grâce à la redondance et à l'isolation logique des services Azure. Pour garantir la résilience, un minimum de trois zones de disponibilité distinctes est présent dans toutes les régions compatibles avec les Availability Zones.

Les sauvegardes logiques (incluant les versions de service et les données client) sont effectuées quotidiennement sur le Data Center principal, garantissant un RPO maximal de 24 heures. Nous conservons les sauvegardes quotidiennes pendant quatorze jours, les sauvegardes hebdomadaires pendant un mois et les sauvegardes mensuelles pendant un an dans le data center principal. Nous conservons les sauvegardes quotidiennes pendant quatorze jours, une sauvegarde hebdomadaire pendant un mois et une sauvegarde mensuelle pendant un an dans le data center principal.

3. Redondance

Les serveurs sont répliqués. Les data centers sont alimentés par deux arrivées électriques indépendantes et équipés d'onduleurs. Des groupes électrogènes disposant de 48 heures d'autonomie garantissent la production d'électricité en cas de défaillance du réseau d'alimentation. Plusieurs boucles de sécurité ont ainsi été mises en place pour éviter toute indisponibilité potentielle. Cette multiplicité de liens permet également à vos données d'emprunter le chemin le plus court et donc de subir les temps de latence les plus faibles. Les serveurs sont également équipés d'une double alimentation et de doubles cartes réseau pour une infrastructure entièrement redondée.

4. Reprise de service

PLAN DE REPRISE D'ACTIVITÉ

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

- Défaillance logique majeure
- Destruction physique des installations d'hébergement

Dans un tel cas, le client est immédiatement notifié et la procédure de reprise est engagée. Une nouvelle infrastructure est recréée dans un data center disponible chez Microsoft Azure. Les données sont restaurées à partir de la dernière version sauvegardée. Comme indiqué précédemment, les sauvegardes complètes (version de service et données client) sont effectuées, stockées et chiffrées une fois par jour sur un stockage distant ; les données ne quittent jamais physiquement leur lieu de stockage. Cela garantit un RPO (Recovery Point Objective) maximal de 24 heures.

La durée maximale du PRA est de 12 heures. Dans le cas d'un changement de data center nécessitant la modification des IP des entrées DNS, les caches DNS dans le monde mettent au plus 24 heures à se mettre à jour.

Cela garantit un RTO (Recovery Time Objective) inférieur à 24 heures.

Pour des informations plus détaillées, veuillez vous reporter au document intitulé :

RÉPONSE EN CAS D'INCIDENT

Chez les hébergeurs de 360Learning

Des alarmes sont configurées pour notifier automatiquement les équipes opérationnelles dès que les premiers signaux d'alerte atteignent les seuils prédéfinis. Une fois un seuil atteint, la procédure de réponse à incident 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.

L'ensemble des événements est documenté et conservé pendant 90 jours après leur observation.

Sur notre réseau

360Learning utilise un système de jeton unique attaché à l'adresse IP afin de 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 de détection d'une attaque, tous les clients concernés sont prévenus dans un délai de 24 heures.

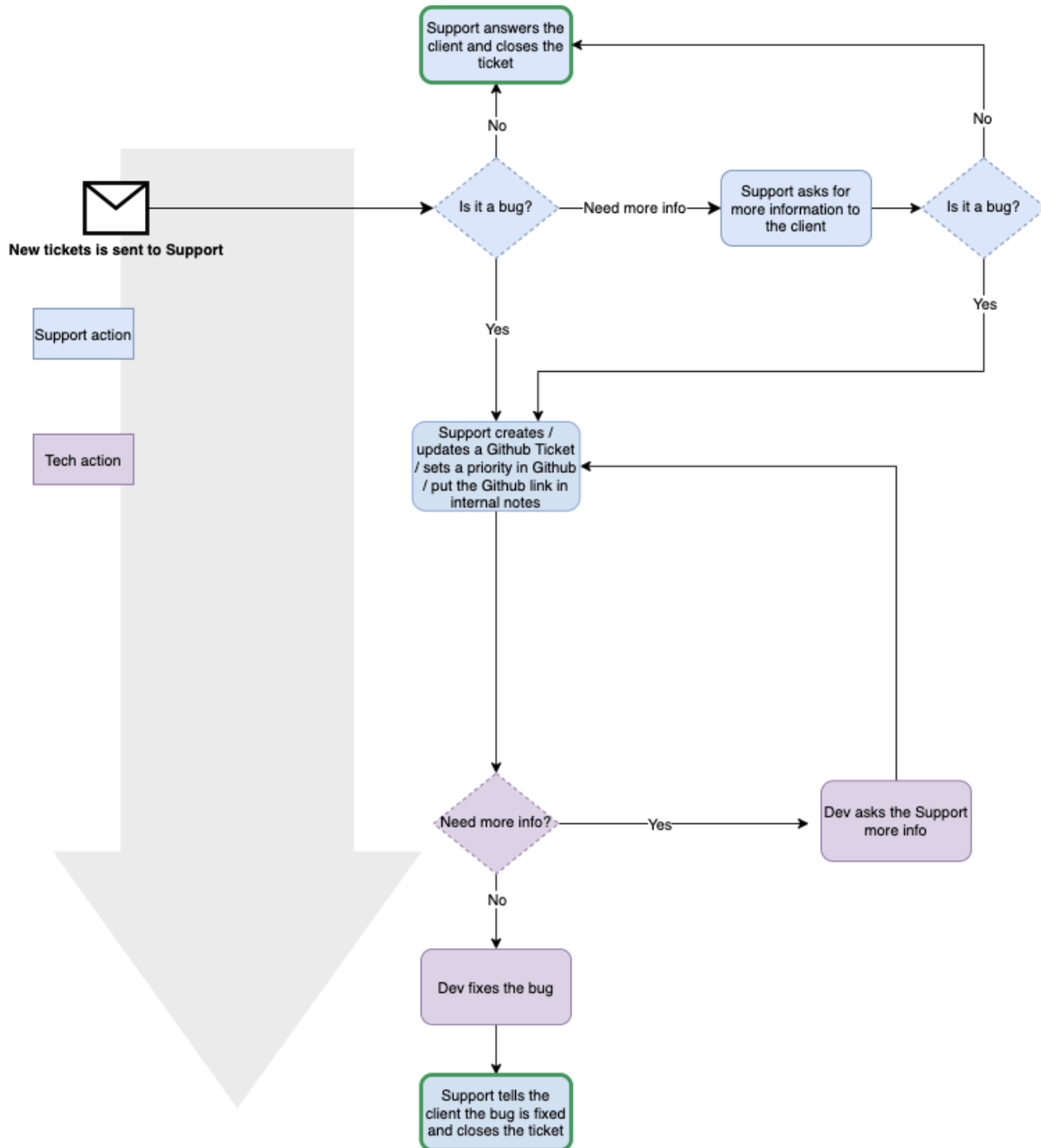
SUPPORT TECHNIQUE

360Learning propose un service de support technique en ligne, accessible en français, anglais et allemand, pendant ses horaires d'ouverture : de 9h00 à 18h00 (heure d'Europe centrale), du lundi au vendredi.

- Support technique et fonctionnel via Zendesk
- Mise à disposition d'une aide en ligne contextuelle
- Accompagnement à l'utilisation de l'API documentée
- Accompagnement aux intégrations SSO

PROCESSUS DE SUPPORT

Ticket funnel



| Scalabilité

1. Occupation système

SAAS (SOFTWARE AS A SERVICE)

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

De ce fait, il ne nécessite aucune installation et est accessible depuis n'importe quel poste connecté à Internet.

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

ARCHITECTURE LOGICIELLE

Notre architecture est constituée de trois couches :

- L'interface, en JavaScript, est exécutée côté client. Elle contient quelques workflows et de la logique métier. Cet élément scale naturellement : chaque client la reçoit dès qu'il se connecte au site, et l'exécute lui-même.

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

- L'API REST, exposée par un serveur web Node.js. Cette API est constituée 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, en pic, que jusqu'à 30 % des ressources CPU et 10 % des ressources RAM.
- Node.js envoie ensuite des requêtes vers une base de données MongoDB pour stocker les données. Une seule réplique suffit actuellement à répondre à toutes les requêtes en lecture et écriture, en utilisant environ 10 % de ses ressources. Une fois 40 % des ressources atteintes, un processus de migration sera engagé pour héberger cette base MongoDB dans le cloud, en utilisant l'une des 3 méthodes standard de sharding de MongoDB (le choix sera fait selon notre profil de charge au moment de la décision de migration). Il s'agit d'une étape standard ne nécessitant que quelques lignes de configuration.

MONITORING

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

Les indicateurs de performance système surveillés par 360Learning sont le CPU, la RAM, l'utilisation disque, les I/O, le réseau, le nombre de requêtes, la latence par service, ainsi que d'autres métriques standard. En complément de ces métriques bas niveau, 360Learning surveille également des indicateurs métier de plus haut niveau, comme le nombre de cours suivis, le nombre de ressources créées (cours, utilisateurs, groupes, parcours, etc.) et bien d'autres. Il n'est pas prévu que les clients y aient accès. 360Learning fournit toutefois en temps réel des statistiques relatives à l'activité des utilisateurs sur les plateformes de ses clients via le dashboard de l'application, qui peut être exporté.

360Learning collecte et stocke les logs d'accès et de requêtes ainsi que les erreurs et incidents. Ces éléments sont stockés, signés et agrégés pour l'ensemble de notre infrastructure et pour tous nos clients. La durée de conservation est fixée à un minimum de 3 mois et un maximum de 6 mois.

TECHNOLOGIES ET OUTILS

360Learning fait usage de technologies de pointe, également adoptées par les principaux acteurs du Web. Parmi celles-ci :

JavaScript & TypeScript

La plateforme 360Learning est développée intégralement en JavaScript. Les bénéfices sont nombreux :

- Le temps de développement est significativement réduit : l'équipe R&D n'a qu'une seule technologie à maîtriser.
- Les temps de chargement sont optimisés : la charge est déportée sur le poste de l'utilisateur, qui ne demande des données que lorsque c'est nécessaire.

Pour une fiabilité encore meilleure, le code est en cours de migration vers TypeScript, un sur-ensemble de JavaScript visant à détecter plus précisément les erreurs et incohérences dans le code et offrant une maintenance facilitée (à la date de rédaction, plus de 80 % des fichiers du code source sont en TypeScript).

Vue.js

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

Node.js

360Learning utilise Node.js, une plateforme logicielle open source orientée événements, conçue pour les applications réseau requérant une forte scalabilité. 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 un système de gestion de base de données orienté documents, MongoDB, une technologie de pointe adaptée à la scalabilité. C'est l'un des SGBD les plus largement utilisés aujourd'hui, notamment par Facebook, LinkedIn, Google ou Amazon.

Systèmes de bases de données plus spécialisés

Pour des fonctionnalités spécifiques, 360Learning s'appuie sur la puissance de systèmes de gestion de données plus adaptés et à la pointe de la technologie, parmi lesquels Elasticsearch, Redis et Snowflake. Ils prennent en charge des fonctionnalités telles que les dashboards, LiveLearners, Recommendations For You, Search, et bien d'autres.

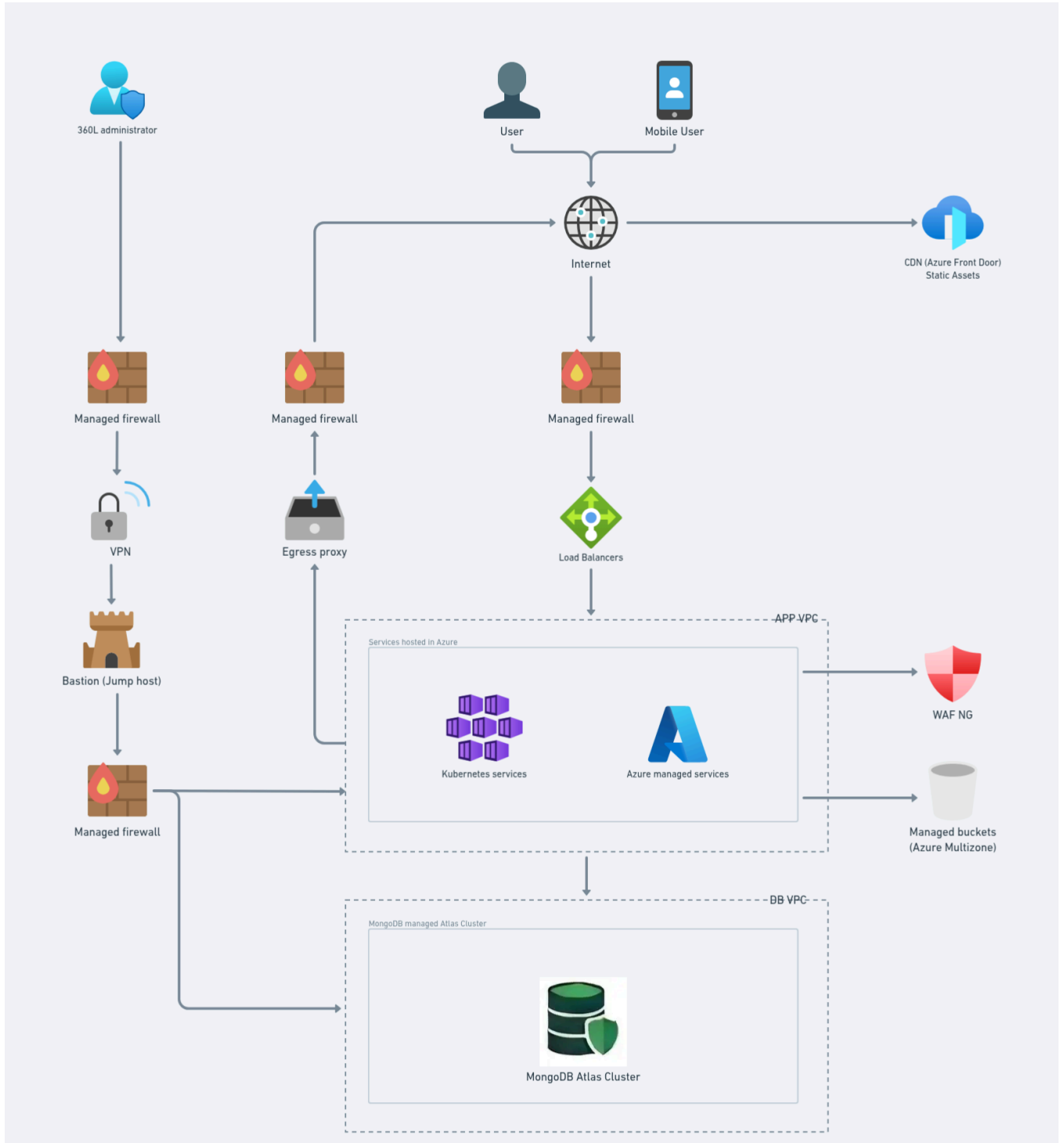
SERVEURS

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 majeure d'un navigateur est publiée, 360Learning s'assure que sa plateforme est compatible.

RÉSEAU



L'ensemble des données est répliqué sur un serveur de pré-production, qui est intégralement testé toutes les 3 semaines. Les temps de réponse du cloud sont régulièrement testés via cinq requêtes prédéfinies. Les temps de réponse depuis la France doivent être inférieurs à 50 ms.

2. Volume client

Afin de garantir un usage équitable pour l'ensemble des utilisateurs, 360Learning documente et met optionnellement en place des limites sur certaines fonctionnalités. Si le client a besoin de plus de 200 000 utilisateurs sur sa plateforme, l'équipe R&D doit en être informée un mois à l'avance afin d'engager un processus de redimensionnement. Une plateforme ne peut excéder 30 000 groupes. Nous appliquons également des [rate limits](#) à l'API 360Learning. Par ailleurs, les limites sur des fonctionnalités spécifiques sont documentées dans la [base de connaissances 360Learning](#).

| Intégrations

1. SSO

OBJECTIFS

Le Single Sign-On (SSO) est un mécanisme d'authentification qui permet aux utilisateurs d'accéder à plusieurs applications avec un unique jeu d'identifiants.

En activant le SSO pour votre application 360Learning, vous devenez responsable de l'authentification de vos utilisateurs : ils sont authentifiés via votre propre portail de connexion et n'ont plus besoin d'un jeu de login/mot de passe supplémentaire.

Les bénéfices de l'utilisation du SSO incluent :

- Une expérience utilisateur améliorée
- Une sécurité renforcée
- Une 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 peut être facilement intégré à votre système d'authentification d'entreprise, par exemple Windows Active Directory.
- JWT est un standard relativement récent basé sur JSON, utilisé dans les protocoles d'authentification les plus récents. Il offre une grande flexibilité.

- OpenID Connect repose sur le protocole OAuth 2.0 et utilise un JSON Web Token (JWT) supplémentaire pour standardiser des aspects laissés au choix par OAuth 2.0, comme les scopes et la découverte de endpoints.

DOCUMENTATION

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

- [360Learning - Guide technique - SSO JWT](#)
- [360Learning - Guide technique - SSO SAML](#)
- [360Learning - Guide technique - SSO OIDC](#)

2. API

OBJECTIFS

L'API 360Learning permet la synchronisation bidirectionnelle d'un annuaire d'utilisateurs avec celui des utilisateurs 360Learning. Vous pouvez facilement ajouter ou retirer des utilisateurs, ainsi que définir leur nom, mot de passe et principales caractéristiques de profil. Vous pouvez ajouter des utilisateurs à des groupes, par exemple pour maintenir les groupes 360Learning à jour avec les évolutions de votre organisation.

L'API permet également d'exporter les statistiques de formation relatives à un programme.

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

DOCUMENTATION

La documentation de l'API est disponible en ligne sur <https://api.360learning.com/>

Un guide technique est également disponible pour vous aider à l'intégrer :

- [360Learning - Guide technique - API](#)

Certaines limitations à connaître sur l'utilisation de l'API sont indiquées sur cette page <https://support.360learning.com/hc/en-us/articles/210620943-Technical-guide-API>,

Si vous avez besoin d'exécuter un nombre élevé de requêtes, nous vous suggérons de cadencer les appels par lots ou en mettant en place un timer dans vos 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 l'API à disposition, ainsi que les droits et obligations associés à son utilisation.

Les API font partie intégrante des Services et ne sont donc accessibles qu'à :

- aux clients d'une entité du groupe 360Learning ayant 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 définie par 360Learning ;
- aux partenaires ayant conclu un contrat avec 360Learning SA, en sa qualité de titulaire des droits sur la plateforme, définissant les modalités d'accès et d'utilisation des API.

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

MODALITÉS ET CONDITIONS D'ACCÈS

Vous accédez à l'API et l'utilisez dans les conditions du contrat conclu avec 360Learning.

Les modalités et limites d'accès sont définies dans le Guide technique API.

Il vous appartient, en qualité de Responsable de traitement, d'utiliser l'API dans le respect des règles relatives à la protection des données à caractère personnel. Vous garantissez à 360Learning que vous utiliserez les API dans le respect des droits des titulaires des systèmes avec lesquels vous mettez en œuvre l'API.

Dans le cas où un tiers accéderait et utiliserait l'API, cette utilisation est effectuée sous votre responsabilité, au seul bénéfice de vos utilisateurs couverts par le contrat conclu entre vous et 360Learning (sociétés affiliées, prestataires de votre système d'information, éditeurs).

Dans ce cadre, l'API vous est mise à disposition à des fins exclusivement techniques et internes. Il est interdit de :

- détourner l'usage de l'API à des fins commerciales ;
- commettre tout acte de contrefaçon, en particulier donner accès, en tout ou en 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 les équipements informatiques utilisés pour accéder à l'API sont conformes à l'état de l'art en matière de sécurité. 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 soupçon légitime de non-respect des conditions d'utilisation de l'API.

PROPRIÉTÉ DE L'API ET CONTINUITÉ

360Learning est titulaire des droits sur l'API et agit en qualité de gestionnaire de l'API.

360Learning peut déprécier, modifier ou limiter l'accès aux API. Dans ce cas, elle en informera les clients sans délai injustifié.

360Learning ne peut être tenue responsable des conséquences de ces modifications, dans la mesure où 360Learning ne s'engage pas sur la continuité des API. En cas de dépréciation, modification ou limitation d'accès entraînant une dégradation significative des Services impactant les conditions déterminantes pour lesquelles le client a souscrit un contrat pour les Services, le client peut résilier le Contrat, sous réserve d'un préavis écrit de trente (30) jours. Sauf objection légitime de 360Learning, la résiliation prend effet à la date d'expiration du préavis notifié par lettre recommandée exposant et démontrant la dégradation significative des Services et le lien direct avec les conditions déterminantes de la contractualisation.

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

Raison sociale du sous-traitant	Localisation d'hébergement des données client	Description des services fournis	Le cas échéant : mécanisme de transfert mis en place pour assurer un niveau de protection adéquat des données à caractère personnel transférées vers un pays tiers a	Données à caractère personnel traitées
Microsoft	France US pour les clients américains*	Hébergement de l'infrastructure de 360Learning Services d'IA générative	N/A	Nom, Prénom, E-mail, Emploi, Photo, Login, Statistiques d'usage et, plus généralement, l'ensemble des données traitées dans le cadre des services.
MongoDB Atlas	France US pour les clients américains*	Hébergement de la base de données MongoDB de 360Learning. Infrastructure fournie par Microsoft Azure	N/A	Nom, Prénom, E-mail, Emploi, Photo, Login, Statistiques d'usage et, plus généralement, l'ensemble des données traitées dans le cadre des services.
Scaleway	France	Hébergement d'environnement de test, pour les clients qui en ont fait la demande pour leurs propres besoins	N/A	Nom, Prénom, E-mail, Emploi, Photo, Login, Statistiques d'usage et, plus généralement, l'ensemble des données traitées dans le cadre des tests

Amazon SES	UE (Irlande) US pour les clients américains*	Envoi des e-mails de notification	N/A	E-mail, Contenu de l'e-mail et Opt-in e-mail
Amplitude (non utilisé pour les clients allemands)**	US	Statistiques d'usage à des fins de reporting	- DPA signé avec Clauses Contractuelles Types (CCT) - Certifié conforme au cadre EU-U.S. Data Privacy Framework	ID (pseudonymisation)
Pendo	UE	Notifications, guides et autres communications in-app de la plateforme.	N/A	ID (pseudonymisation)
Datadog	UE	Observabilité	N/A	ID (pseudonymisation)
Snowflake Computing Netherlands B.V.	UE US pour les clients américains*	Statistiques d'usage à des fins de reporting, Mise à disposition de fonctionnalités de traitement de données (ex. : recherche dans la plateforme)	N/A	Nom, Prénom, E-mail (afin de les rendre disponibles dans la recherche - Non utilisés pour les statistiques) - Pour les statistiques : ID (pseudonymisation)
Elastic App Search	UE US pour les clients américains*	Moteur de recherche pour la recherche dans la plateforme ; analytics d'usage pour les recommandations	N/A	Nom, Prénom, E-mail
Workato	UE pour les clients EMEA - US pour les clients américains*	Fournisseur iPaaS pour les automatisations et les intégrations tierces	N/A	Uniquement pour les connecteurs Workato : données à caractère personnel chargées dans le service, qui peuvent inclure, sans s'y limiter : Nom, Prénom, E-mail.
Les sous-traitants autorisés suivants ne peuvent avoir accès qu'à un nombre limité d'utilisateurs autorisés disposant d'un rôle spécifique : Auteur, Administrateur, Owner				
Zendesk	UE***	Gestion des demandes de support client	- DPA signé avec Clauses Contractuelles Types (CCT) - Certifié conforme au cadre EU-U.S. Data Privacy Framework	Nom, Prénom, E-mail, Photo (si renseignée)

* Pour les clients américains ayant signé un contrat avec 360Learning INC et ayant expressément demandé que leurs données soient stockées dans des data centers américains.

** Pour les clients allemands ayant signé un contrat avec 360Learning GmbH.

*** Dans des circonstances exceptionnelles et pour assurer un support efficace en cas de réception d'un nombre élevé de demandes, des opérateurs américains peuvent prendre en charge des clients EMEA, et des clients américains peuvent être pris en charge par des opérateurs UE.

Afin de fournir le meilleur service à nos clients, cette liste est susceptible d'évoluer.

Pour plus d'informations sur le traitement des données à caractère personnel, nous vous invitons à consulter notre politique de confidentialité accessible via 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, ce qui signifie qu'ils sont nécessaires à la fourniture des services. Leur traitement est fondé sur l'intérêt légitime, conformément au RGPD, et ne nécessite pas de consentement spécifique.

Vous trouverez ci-dessous la description de ces cookies fonctionnels :

Nom du cookie	Usage du cookie	Données à caractère personnel traitées par le cookie	Durée de conservation du cookie	Parti e***	Pays du service associé au cookie
refreshToken	Identifiant utilisé pour obtenir un nouveau jeton lorsque le jeton initial (15 minutes) expire	N/A	30 jours	1st	FR/US*
signToken	Jeton utilisé pour créer/activer un utilisateur	N/A	30 jours	1st	FR/US*
linkTokenError	Stocke un message d'erreur lorsqu'un lien (invitation/réinitialisation) échoue à la validation. Valeurs : "expiredLink", "alreadyActiveUser", "invalidLink"	N/A	30 s	1st	FR/US*
tempToken	Jeton temporaire pour le SSO afin d'assurer le fonctionnement avec une version spécifique de Safari	N/A	session	1st	FR/US*
token	Jeton JWT pour l'authentification (HTTP only)	N/A	15 minutes	1st	FR/US*
unauthorizedIp	Affiche un message d'erreur spécifique lorsque l'IP n'est pas autorisée	N/A	session	1st	FR/US*
oidc_code_verifier	Vérificateur de code PKCE pour le flux d'authentification OpenID Connect	N/A	10 minutes	1st	FR/US*
oidc_nonce	Nonce OIDC pour prévenir les attaques par rejeu de jeton	N/A	10 minutes	1st	FR/US*

oidc_state	Paramètre state OIDC pour la protection CSRF lors du flux d'autorization code	N/A	10 minutes	1st	FR/US*
mobileApplInstalle d	Indique si l'application mobile est installée sur l'appareil. Utilisé pour décider entre rediriger vers l'application ou rester dans le navigateur.	N/A	30s	1st	FR/US*
skipMobileRedirection	Lorsque la valeur est "true", désactive la redirection automatique vers l'application mobile.	N/A	30s	1st	FR/US*
amplitude_id_xxxx xxxxxxxxxxx	Notre partenaire de système de tracking Amplitude — données utilisées uniquement par 360Learning	ID (pseudonymisé)	1 an	2nd	USA**
AMP_xxx	Autres cookies déposés par notre partenaire Amplitude	ID (pseudonymisé)	1 an	2nd	USA**
_dd_s	Notre partenaire de logging d'erreurs front-end Datadog	ID (pseudonymisé)	1 an	2nd	USA**

* Les cookies restent dans le pays où la plateforme est utilisée : France (FR) pour l'usage de la plateforme EMEA, et États-Unis pour l'usage de la plateforme NA.

** Pays partiellement adéquat. Amplitude est membre du EU-US Data Privacy Framework. Des mesures complémentaires de protection des données à caractère personnel ont été mises en place, telles que la souscription à un DPA conforme et aux clauses contractuelles types de la Commission européenne.

*** 1st (HostOnly=true) / 2nd (HostOnly=false)

Dans certains cas spécifiques, 360Learning peut agir en qualité de Responsable de traitement, par exemple lorsqu'elle collecte et traite des données à caractère personnel à des fins de gestion commerciale et administrative auprès des clients et de leurs collaborateurs. Des statistiques d'usage pseudonymisées sont également collectées afin de permettre l'analyse et l'amélioration de nos services. 360Learning peut être amenée, à des fins exclusives d'administration et de gestion, à partager ces données à caractère personnel avec ses prestataires et/ou ses sociétés affiliées.

360Learning prend toutes les précautions nécessaires lors de la collecte et du traitement des données à caractère personnel 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 à caractère personnel du client sont conservées pendant une durée conforme aux dispositions légales et proportionnée aux finalités pour lesquelles elles ont été enregistrées. Lorsque la conservation n'est plus justifiée par des exigences légales ou commerciales, ou par la gestion du compte du client, ou si le client exerce l'un de ses droits tels que le droit d'opposition ou d'effacement, nous procéderons à la suppression sécurisée des données.

Politique de modération

Les présentes règles d'utilisation ont pour objet de définir les principes et procédures 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 relatif aux services numériques du 19 octobre 2022 (« DSA »), au titre duquel 360Learning est qualifiée d'« hébergeur ». Les présentes dispositions ne dispensent pas les Clients de leur obligation d'insérer leur propre charte de modération sur la plateforme, à destination de leurs utilisateurs.

Principes généraux applicables à l'utilisation de la plateforme 360Learning :

Lorsqu'ils utilisent la plateforme 360Learning, les Clients et Bénéficiaires doivent respecter les principes généraux suivants :

- Respect de la loi : tout contenu publié sur la plateforme 360Learning doit respecter la réglementation applicable, notamment les 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, y compris en cas de désaccord. Ils doivent s'abstenir de tout langage haineux, discriminatoire ou offensant ;
- Les commentaires dans le forum doivent porter uniquement sur les échanges relatifs aux contenus dans le cadre du Collaborative Learning ;
- Confidentialité et vie privée : le partage d'informations personnelles d'autres utilisateurs sans leur consentement est strictement interdit ;
- Authenticité et propriété intellectuelle : les utilisateurs doivent s'assurer que les contenus qu'ils publient sont authentiques et qu'ils détiennent les droits de propriété intellectuelle nécessaires ;
- Véracité de l'information : la diffusion d'informations fausses ou de contenus trompeurs est strictement interdite.

Responsabilité concernant les 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 à et l'utilisation d'une plateforme permettant aux Clients et Bénéficiaires de créer une expérience de formation engageante et collaborative, par la création et la mise à jour de contenus de formation à des fins pédagogiques.

Les Clients, qui sont responsables des contenus publiés sur la plateforme, sont tenus de publier leur propre charte de modération des contenus. 360Learning, en sa qualité d'hébergeur, peut suspendre ou supprimer les contenus considérés comme illicites au regard de la législation applicable ou figurant dans la liste suivante :

Catégories de contenus illicites :

- Contenus illicites : contenus contraires au droit français et européen, tels que les discours de haine, l'apologie du terrorisme, la pédopornographie, etc. ;
- Contenus haineux ou discriminatoires : contenus incitant à la haine, à la violence ou exerçant une discrimination à l'encontre d'une personne ou d'un groupe de personnes en raison de son origine, de sa religion, de ses opinions politiques, etc. ;
- Contenus portant atteinte à la vie privée : contenus divulguant des informations personnelles sans le consentement de la personne concernée ;
- Contenus à caractère sexuel : contenus pornographiques ou sexuellement explicites, y compris la représentation de mineurs ;
- Contenus faux ou trompeurs : contenus diffusant de fausses informations ou de nature à induire les utilisateurs en erreur ;
- Contenus plagiés : contenus sur lesquels l'utilisateur qui les publie ne dispose d'aucun droit de propriété intellectuelle.

Signalement au client :

Il est rappelé aux Clients qu'ils sont responsables des contenus publiés sur la plateforme, et qu'il leur incombe de les valider avant leur partage.

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 définie par le client.

Pour plus de détails sur cette procédure, veuillez consulter cet article : [Charte de modération](#)

Signalement de 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 : [Signalement de commentaires](#)

Mécanisme de signalement de contenus illicites à 360Learning, agissant en qualité d'hébergeur :

01. Report content via data-protection@360Learning.com
02. 360Learning will send an acknowledgement of receipt within 30 days of receiving the report.
03. The 360Learning team of moderators will handle the report as quickly as possible.
04. The person who filed the report will be notified of the decision taken following the processing of the report.
05. **In the event of a positive response, the content in question is removed from the platform.**
A notification is sent to the person having published the illicit content, with a statement of the reasons and the means to appeal the decision.

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 signalement doit contenir au minimum :

- Les coordonnées de la personne effectuant le signalement ;
- Les coordonnées de l'entité fournissant l'accès à la plateforme (le Client) ;
- Le lien URL et toute autre information sur la localisation du contenu ;
- Les motifs pour lesquels le contenu est considéré comme illicite.

360Learning adressera un accusé de réception à la personne effectuant le signalement dans un délai de 30 jours à compter de la réception du signalement.

Les signalements de contenus adressés à 360Learning seront traités par l'équipe de modérateurs de 360Learning dans les meilleurs délais.

La personne effectuant le signalement sera notifiée de la décision prise à l'issue du traitement du signalement.

En cas de réponse positive au signalement, le contenu en question sera retiré 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 l'exposé des motifs de la décision et des voies de recours permettant de contester la décision de restreindre le contenu à l'issue du traitement du signalement

Conformément à ses obligations au titre du DSA, 360Learning a désigné data-protection@360Learning.com comme point de contact pour toutes les communications.