MINISTÈRE
DE L'ENSEIGNEMENT
SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'ESPACE

Liberté
Égalité
Fraternité

Charte d'usage du Système d'information Parcoursup

Préambule

La sécurisation des données du système d'information Parcoursup, la performance des traitements et la protection des données personnelles des utilisateurs sont des enjeux essentiels pour le Ministère de l'enseignement supérieur, de la recherche et de l'espace, les rectorats et l'ensemble des établissements scolaires ou d'enseignement supérieur qui participent à la procédure nationale de préinscription dans le 1er cycle de l'enseignement supérieur. Elle participe de la confiance dans le système d'information et les informations dont il assure la gestion.

Face aux risques accrus de cyber malveillance, des mesures de sécurité et de vigilance sont prises par le SCN Parcoursup pour renforcer la sécurité numérique, notamment celle des comptes utilisés par les usagers en administration centrale, dans les administrations déconcentrées et en établissements scolaires et d'enseignement supérieur.

Il est rappelé que la sécurité numérique est l'affaire de tous. Chaque utilisateur peut agir pour limiter les risques : robustesse et protection des mots de passe, usage exclusif de chaque compte par une seule personne, utilisation d'équipements professionnels protégés par les antivirus mis à disposition par l'institution de rattachement, gestion raisonnée des délégations.

Contexte

La plateforme Parcoursup est désignée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en tant qu'opérateur de service essentiel (OSE) au titre de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

Le Service à compétence nationale (SCN) Parcoursup applique notamment :

- Les règles de sécurité prévues par le décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et l'arrêté du 14 septembre 2018 fixant les règles de sécurité relatives à la sécurité des réseaux et systèmes d'informations des opérateurs de services essentiels.
- Les règles de sécurité prévues par l'arrêté du 13 juin 2014 (modifié par l'arrêté du 10 juin 2015) portant approbation du référentiel général de sécurité (RGS) ;
- Les règles de protection des données personnelles prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ainsi que le règlement européen relatif « à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données » [UE 2016/679] ;

A ce titre, le SCN Parcoursup met en œuvre des dispositifs de contrôle et de surveillance afin :

- De protéger les technologies et les informations de l'administration et des utilisateurs contre les actes illicites ou de malveillance ;
- D'assurer la sécurité du système d'information ;
- De permettre leur emploi pour des usages professionnels dans des conditions optimales.

Ces mesures peuvent prendre la forme :

- De dispositifs de gestion des droits d'accès et des habilitations des utilisateurs du système d'information ;
- De contrôles automatisés de prévention contre l'usurpation d'identité, de prévention contre la fuite d'informations et de suppression des comptes inutilisés. Les blocages qui pourraient en résulter sont explicités dans la mesure du possible par des messages d'information à l'utilisateur ;
- De dispositifs de collecte de données et de traces,
- D'un système de journalisation des accès à la plateforme.

Ces dispositifs sont mis en œuvre conformément au cadre légal et réglementaire en vigueur, et le cas échéant aux déclarations effectuées auprès de la Commission nationale de l'informatique et des libertés (CNIL), notamment la durée de conservation des traces.

Objet de la charte

La présente Charte définit les règles d'usage et de sécurité applicables pour l'usage du système d'information Parcoursup : elle précise les droits et devoirs de chacun pour un usage nominal de la plateforme numérique. Elle est applicable à toute personne physique, dénommée l'« utilisateur » dans la suite du document, ayant accès, dans le cadre de l'exercice de son activité professionnelle aux ressources du système d'information Parcoursup.

La présente charte s'applique immédiatement à tout utilisateur du système d'information Parcoursup et pourra faire l'objet de révisions, en fonction des évolutions technologiques et juridiques du Système d'Information et de ses impératifs de sécurité.

Engagements de l'utilisateur

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information Parcoursup. Il a une obligation de réserve et de confidentialité à l'égard des informations et des documents auxquels il accède.

Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie.

L'utilisateur veille notamment à :

- Ne communiquer ou ne partager en aucun cas ses identifiants, mots de passe ou clés d'authentification à qui que ce soit, y compris à l'assistance informatique ;
- Utiliser des moyens d'authentification professionnels distincts des mots de passe utilisés pour des usages privés ;
- Changer régulièrement ses mots de passe ;
- Assurer la mise à jour régulière des systèmes d'exploitation et des logiciels de sécurité (antivirus)sur son poste de travail ;

- Signaler à sa hiérarchie dans les meilleurs délais toute anomalie découverte telle une intrusion dans le système d'information, une infection de son poste, etc. ;
- Ne pas effectuer d'actions telles que la diffusion, le stockage, ou toute action similaire concernant les données obtenues à travers le système d'information Parcoursup, sur tout support non reconnu comme sécurisée par le référent SSI de son établissement.

Règles de sécurité informatique

Les codes d'accès au système Parcoursup : login et mot de passe

Chaque compte Parcoursup est strictement personnel et nominatif.

Tout utilisateur est informé que ses codes d'accès à Parcoursup constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Les niveaux d'accès ouverts à l'utilisateur sont définis par son administrateur en fonction de la mission qui lui est conférée.

L'administrateur Parcoursup limite donc l'accès à chaque utilisateur aux ressources pour lesquelles il est expressément habilité. L'administrateur met à jour les comptes et les droits des utilisateurs de son périmètre et veille notamment à la suppression des compte non utilisés.

La sécurité du système Parcoursup mis à sa disposition impose à chaque utilisateur :

- De respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès ;
- De garder strictement confidentiel son code d'accès à la plateforme et de ne pas le dévoiler à un tiers ;
- De respecter la gestion des accès, en particulier de ne pas utiliser les codes d'accès d'un autre utilisateur, ni de chercher à les connaitre.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite la mise en place d'un process de double authentification mise en œuvre sur détection d'une adresse IP inconnue pour un utilisateur et au moyen d'une récupération de code unique (OTP, One Time Password) par sms, mail ou application dédiée.

Protection des données personnelles

Les données récupérées par les établissements de formation dans le cadre de la procédure Parcoursup constituent des données personnelles au sens du règlement général sur la protection des données (RGPD) du 27 avril 2016 applicable en France depuis le 25 mai 2018.

L'utilisation de ces données pour les besoins de l'examen des vœux prescrit par la procédure nationale de préinscription obéit donc aux règles concernant d'une part, la déclaration du traitement et l'information sur le traitement de données et, d'autre part, la protection des données prévues par ledit RGPD.

J'ai pris connaissance des dispositions de la charte relative à la sécurité numérique et la protection des données personnelles.