Annexe 5
Sécurité des données et base du rapport ISAE 3000 de SIX

pour le contrat de participation à la plate-forme bLink

La présente annexe décrit la sécurité des données de la plate-forme et des services fournis par SIX aux participants. Les objectifs d'audit énumérés sont basés sur la norme internationalement reconnue «Information Security Forum (ISF) – The Standard of Good Practice for Information Security 2018» et sont divisés en différents domaines d'audit. Les objectifs de contrôle énumérés ci-dessous constituent la base de la sélection des contrôles pour le rapport annuel ISAE 3000 de type II.

N°	Déclaration	Description	Réf (ISF)
1	Gouvernance de la sécurité		
1.1	Cadre de gouvernance de la sécurité	SIX dispose d'un cadre pour la gouvernance de la sécurité de l'information; l'engagement y est démontré par l'organe directeur de l'organisation.	SG.01.01.01
1.2	Direction de la sécurité	SIX dispose d'un responsable de la sécurité à plein temps au niveau de la direction générale, auquel incombe la responsabilité globale du programme de sécurité de l'information de l'organisation.	SG.01.02.01
2	Évaluation des risques liés à l'information		
2.1	Cadre/méthodologie de l'évaluation des risques liés à l'information	SIX dispose d'une procédure documentée pour la gestion des évaluations des risques liés à l'information. Les évaluations des risques sont basées sur une méthodologie structurée et systématique d'évaluation des risques liés à l'information.	IR.01.01.01 IR.01.02.01
3	Gestion de la sécurité		
3.1	Politique de sécurité de l'information	SIX dispose d'une politique de sécurité de l'information documentée qui s'applique à l'ensemble de l'organisation et qui est communiquée à toutes les personnes ayant accès aux informations et aux systèmes de l'organisation.	SM.01.01.01
3.2	Politiques d'utilisation acceptable	SIX dispose d'un règlement qui définit la manière dont les personnes sont censées utiliser les informations et les systèmes au sein de l'organisation.	SM.01.02.01
3.3	Fonction de sécurité de l'information	SIX dispose de partenaires à la sécurité de l'information dédiés pour les unités commerciales, dirigées par le responsable de la sécurité, qui ont la responsabilité de promouvoir les bonnes pratiques en matière de sécurité de l'information dans toute l'organisation.	SM.02.01.01
4	Gestion du personnel		
4.1	Cycle de vie professionnelle	SIX procède à une présélection des candidats avant le début du travail (par exemple en reprenant les références, en vérifiant l'historique de la carrière/les qualifications et en confirmant l'identité, par exemple par l'inspection d'un passeport). Dans le cas de fonctions particulièrement critiques en matière de sécurité, les collaborateurs sont régulièrement contrôlés en ce qui concerne les facteurs de risque et en cas d'accès aux données d'identification des clients, un extrait du casier judiciaire et du registre de recouvrement des créances doit être obtenu.	PM.01.01.01
4.2	Propriété et responsabilités	Au sein de SIX, la propriété d'environnements d'entreprise, de processus et d'applications critiques (y compris l'infrastructure technique de support) est attribuée à des personnes individuelles (par exemple des directeurs d'entreprise), reconnue et documentée.	PM.01.02.01
4.3	Programme de sensibilisation à la sécurité	SIX dispose d'un programme de sensibilisation à la sécurité visant à promouvoir et à intégrer les comportements attendus en matière de sécurité dans toute l'organisation et à établir une culture en matière de sécurité positive. Les employés de SIX reçoivent régulièrement des formations sur différents sujets liés à la sécurité.	PM.02.01.01
5	Gestion de l'information		
5.1	Classification et traitement de l'information	SIX dispose d'un système de classification des informations (soutenu par des lignes directrices sur le traitement des informations) qui s'applique dans l'ensemble de l'organisation et qui est basé sur la confidentialité des informations.	IM.01.01.01 IM.02.02.01

5.2	Confidentialité des informations	SIX dispose d'un responsable de la protection des données qui est chargé de gérer les contrôles de confidentialité et de sécurité des informations appliqués au traitement des informations personnelles identifiables (c'est-à-dire les informations qui peuvent être utilisées pour identifier une personne).	IM.01.02.01
6	Gestion des actifs physiques		
6.1	Gestion du cycle de vie du matériel	SIX dispose de normes/procédures documentées pour la gestion du cycle de vie du matériel.	PA.01.01.01
7	Informatique mobile		
7.1	Protection des appareils mobiles	Les appareils mobiles de SIX (y compris les ordinateurs portables, les tablettes et les smartphones) sont construits selon des configurations techniques standard et soumis à des pratiques de gestion de la sécurité afin de protéger les informations contre la perte, le vol et la divulgation non autorisée. Ils sont également dotés de moyens sécurisés pour se connecter à d'autres appareils et à des réseaux.	PA.02.01.01 PA.02.03.01
7.2	Dispositifs de stockage portables	SIX dispose de normes/procédures documentées couvrant l'utilisation des dispositifs de stockage portables.	PA.02.05.01
8	Développement de système		
8.1	Méthodologie de développement de système	Les activités de développement de SIX sont menées conformément à une méthodologie de développement de système documentée.	SD.01.01.01
8.2	Environnements de développement de système	Les activités de développement de système de SIX sont réalisées dans des environnements de développement spécialisés, qui sont isolés des environnements de vie et de test, et protégés contre tout accès non autorisé.	SD.01.02.01
8.3	Spécifications des exigences	Les exigences du système (y compris celles relatives à la sécurité de l'information) de SIX sont documentées dans les exigences opérationnelles et convenues avant le début de la conception détaillée. Les exigences en matière de sécurité de l'information pour les systèmes en cours de développement doivent être prises en compte lors de la conception des systèmes.	SD.02.01.01
8.4	Conception du système	Les exigences en matière de sécurité de l'information pour les systèmes en cours de développement sont prises en compte lors de la conception des systèmes.	SD.02.02.01
8.5	Acquisition de logiciels	SIX dispose de normes/procédures documentées pour l'acquisition de logiciels.	SD.02.03.01
8.6	Test du système	Les systèmes en cours de développement (y compris les progiciels d'application, les logiciels système, le matériel, les communications et les services) sont testés dans une zone de test dédiée qui simule l'environnement réel, avant que le système ne soit promu à l'environnement réel.	SD.02.05.01
8.7	Tests de sécurité	Les systèmes en cours de développement sont soumis à des tests de sécurité en utilisant une série de types d'attaques (y compris des évaluations de vulnérabilité, des tests de pénétration et des tests de contrôle d'accès).	SD.02.06.01
8.8	Critères de promotion du système	Des critères rigoureux (y compris les exigences de sécurité) sont respectés avant que les nouveaux systèmes ne soient promus à l'environnement réel. Les nouveaux systèmes sont installés dans l'environnement réel conformément à un processus d'installation documenté.	SD.02.07.01
8.9	Désaffectation du système	Les systèmes qui ne sont plus nécessaires devraient être évalués et soumis à un processus de désaffectation (le cas échéant), en tenant compte des informations, logiciels, services, équipements et dispositifs pertinents.	SD.02.10.01
9	Gestion des applications commerciales		
9.1	Registre des applications commerciales	Les applications commerciales de SIX sont enregistrées dans un registre des applications commerciales précis et à jour.	BA.01.01.01

9.2	Protection des applications commerciales	Les applications commerciales de SIX sont protégées par l'utilisation de principes d'architecture de sécurité solides.	BA.01.02.01 BA.01.04.01
10	Accès au système		
10.1	Contrôle d'accès	SIX a mis en place un processus de gestion des accès qui réglemente l'accès (y compris la révision périodique) aux applications, systèmes, réseaux et dispositifs informatiques de l'entreprise par tous les types d'utilisateurs.	SA.01.01.01
10.2	Dispositions relatives à l'accès des clients	SIX dispose de normes/procédures documentées pour la fourniture d'un accès aux applications commerciales de l'organisation par les clients.	SA.02.01.01
10.3	Connexions des clients	SIX dispose de normes/procédures documentées pour établir les dispositions techniques de sécurité pour les connexions des clients.	SA.02.03.01
11	Gestion du système		
11.1	Installations informatiques et réseaux	Les systèmes informatiques, les réseaux et les installations de télécommunication (par exemple les centres de données) sont conçus pour répondre aux besoins actuels et futurs en matière de traitement de l'information et sont protégés par une série de contrôles de sécurité intégrés.	SY.01.01.01
11.2	Configuration du serveur	Les serveurs sont configurés conformément à des normes/procédures documentées.	SY.01.02.01
11.3	Accords de niveau de service	Les services informatiques et de réseau qui soutiennent les applications et les processus commerciaux critiques sont définis dans des accords de service documentés (par exemple, des contrats ou des accords sur les niveaux de service) qui répondent aux exigences opérationnelles, de sûreté et de sécurité.	SY.02.01.01
11.4	Sauvegarde	Les sauvegardes des informations et des logiciels essentiels sont effectuées suffisamment fréquemment pour répondre aux besoins des entreprises.	SY.02.03.01
11.5	Gestion des changements	Les modifications apportées aux applications commerciales, aux systèmes d'information et aux dispositifs de réseau sont testées, examinées et appliquées à l'aide d'un processus de gestion des changements.	SY.02.04.01
12	Réseaux et communications		
12.1	Gestion du réseau	Les dispositifs de réseau de SIX sont configurés pour fonctionner selon les besoins et pour empêcher les mises à jour non autorisées ou incorrectes. Les dispositifs de réseau sont physiquement protégés.	NC.01.01.01 NC.01.02.01
12.2	Accès sans fil	Les accès sans fil de SIX sont soumis à une autorisation, à l'authentification des utilisateurs et des dispositifs informatiques, et au cryptage du trafic sans fil.	NC.01.03.01
12.3	Connexions aux réseaux externes	Toutes les connexions externes aux systèmes et aux réseaux sont identifiées, vérifiées, enregistrées et approuvées individuellement par le propriétaire du système ou du réseau.	NC.01.04.01
13	Communications électroniques		
13.1	E-mail/collaboration	Les systèmes d'e-mail et les plates-formes de collaboration sont protégés par une combinaison de contrôles de politique, de sensibilisation, de processus et de sécurité technique.	NC.02.01.01 NC.02.02.01
14	Gestion de la chaîne d'approvisionnement		
14.1	Processus de gestion des fournisseurs externes	SIX dispose d'un processus documenté pour gérer les risques d'information associés aux fournisseurs externes (y compris les organisations de la chaîne d'approvisionnement).	SC.01.01.01
15	Gestion de la sécurité technique		
15.1	Activités de protection contre les logiciels malveillants	Des activités sont menées pour sensibiliser les utilisateurs aux risques liés aux logiciels malveillants et pour préciser les actions nécessaires pour réduire ces risques au minimum.	TS.01.02.01

15.2	Logiciels de protection contre les logiciels malveillants	Les systèmes de toute l'organisation sont protégés contre toutes les formes de logiciels malveillants, un logiciel de protection contre les logiciels malveillants qui est soutenu par des procédures efficaces de gestion des incidents de sécurité liés aux logiciels malveillants étant maintenu à jour.	TS.01.03.01
15.3	Détection d'intrusion	Les mécanismes de détection des intrusions sont utilisés pour les réseaux ayant des applications et des systèmes commerciaux critiques afin d'identifier des types d'attaques prédéterminés et nouveaux.	TS.01.05.01
16	Cryptographie		
16.1	Solutions cryptographiques	Les solutions cryptographiques sont soumises à approbation, documentées et appliquées dans toute l'organisation.	TS.02.01.01
16.2	Gestion des clés cryptographiques	SIX dispose de normes/procédures documentées pour la gestion des clés cryptographiques.	TS.02.02.01
17	Gestion des threats et des incidents		
17.1	Gestion des vulnérabilités techniques	SIX dispose d'un processus d'identification et de correction des vulnérabilités techniques des applications, systèmes, équipements et dispositifs de l'entreprise.	TM.01.01.01
17.2	Enregistrement des événements de sécurité	Les événements importants liés à la sécurité sont enregistrés dans des journaux, stockés de manière centralisée, protégés contre toute modification non autorisée et analysés régulièrement.	TM.01.02.01 TM.01.03.01
18	Gestion des incidents de sécurité		
18.1	Cadre de gestion des incidents de sécurité	Un cadre de gestion des incidents de sécurité de l'information est établi, comprenant les personnes, les informations et les outils pertinents requis par le processus de gestion des incidents de sécurité de l'information de l'organisation.	TM.02.01.01
18.2	Correctifs d'urgence	SIX dispose de normes/procédures documentées pour l'application de correctifs d'urgence aux informations commerciales, aux applications commerciales et aux infrastructures techniques (y compris les logiciels de systèmes et le matériel informatique)	TM.02.03.01
19	Sécurité physique et environnementale		
19.1	Protection physique	Toutes les installations critiques (y compris les lieux qui abritent des infrastructures techniques critiques, des systèmes de contrôle industriel et des équipements spécialisés) sont physiquement protégées contre les accidents ou les attaques et contre l'accès physique non autorisé.	LC.02.01.01
20	Gestion de la continuité des activités		
20.1	Programme de continuité des activités	Un programme de continuité des activités est établi, qui comprend le développement d'une infrastructure technique résiliente, la création d'une capacité de gestion des crises, ainsi que la coordination et le maintien des plans et des dispositions de continuité des activités dans toute l'organisation.	BC.01.02.01
20.2	Gestion de crise	Un processus de gestion de crise doit être établi, soutenu par une équipe de gestion de crise, qui détaille les mesures à prendre en cas d'incident majeur ou d'attaque grave.	BC.01.04.01
20.3	Planification de la continuité des activités	Des plans de continuité des activités sont élaborés et documentés pour soutenir les processus opérationnels critiques dans toute l'organisation.	BC.02.01.01
21	Surveillance et amélioration de la sécurité		
21.1	Gestion de l'audit de sécurité	Des audits de sécurité indépendants sont effectués régulièrement pour les environnements cibles qui sont essentiels au succès de l'organisation.	SI.01.01.01
22	Critères d'admission (Règlement interne de SIX)		
22.1	Audit d'admission	SIX dispose d'un processus documenté qui définit la procédure pour les audits d'admission initiaux ou répétés des participants à la plate-forme et vérifie les critères d'admission conformément au contrat de participation.	N/A