EMEA
MESURES TECHNIQUES ET ORGANISATIONNELLES (MTOs)

Changement de version/révision de l'historique

Communiqué/Version	Date	Auteur(s)	Détails des révisions
1.0	25.05.2018	Gerhard Smischek	Document original
2.0	01.02.2021	Matthew Leszczynski	Passage à un nouveau format de modèle. Passage à la nomenclature commune. Passage au concept de programme de certification ISO/IEC 27001:2013 et Exela ISO 27001. Extension à l'ensemble de l'EMEA.
2.1	19.05.2021	Bernhard Hofmann	Corrections linguistiques pour la version allemande
2.2	20.05.2021	Oleg Simanic	Approbation
3.0	21.07.2021	Mateusz Leszczynski	Mise à jour du périmètre territorial : suppression de 2 locaux fermés, ajout d'un local nouvellement certifié ; Approbation

Préambule

Exela Technologies (ci-après dénommée "Exela") est un leader dans le domaine de l'automatisation des processus d'entreprise, qui s'appuie sur une présence mondiale et une technologie exclusive pour fournir des solutions de transformation numérique améliorant la qualité, la productivité et l'expérience de l'utilisateur final. L'activité d'Exela, qui entre dans le cadre du présent document, est la conception, le développement, la mise en œuvre et le soutien de la gestion de documents et du traitement d'images, la capture de données, les solutions de flux de travail, les services de soutien logiciel et les services gérés, y compris l'impression, le courrier et l'expédition.

Exela entend maintenir la sécurité des données personnelles conformément au RGPD et au RU-RGPD et garantit que les données des clients seront traitées de manière sûre. Le document suivant présente les mesures techniques et organisationnelles appropriées dont le niveau de protection correspond de manière adéquate aux risques des activités de traitement d'Exela. La gestion de la sécurité de l'information décrit les contrôles qu'une organisation doit mettre en œuvre pour s'assurer qu'elle protège raisonnablement la confidentialité, la disponibilité et l'intégrité des actifs contre les menaces et les vulnérabilités.

Les mesures qui ont été prises sont celles qui assurent un niveau de protection adapté au risque en ce qui concerne la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes. L'état de l'art, les coûts de mise en œuvre et la nature, la portée et les objectifs du traitement ainsi que la probabilité et la gravité variables du risque pour les droits et libertés des personnes physiques au sens du RGPD et du RU-RGPD ont été pris en compte. À des fins d'orientation, il est fait référence aux concepts de la norme ISO/IEC 27001:2013 "Systèmes de gestion de la sécurité de l'information", annexe A.

Champ d'application territorial

Les MTO suivantes sont applicables pour la région EMEA et se réfèrent aux locaux d'Exela certifiés ISO/IEC 27001:2013 énumérés ci-dessous :

1. Exela Technologies, Baronsmede House, 20 the Avenue, Egham, TW20 9AB, Royaume-Uni ;
2. Exela Technologies, Sandringham House, Sandringham Avenue, Harlow Business Park, Harlow CM19 5QS, Royaume-Uni ;
3. Exela Technologies, Barclays House, 1 Wimborne Road, Poole BH15 2BB, Royaume-Uni ;
4. Exela Technologies, Moulton House, 10 Pond Wood Close, Moulton Park, Northampton NN3 6DF, Royaume-Uni ;
5. Exela Technologies, 8 Beckett Way, Park West, Nangor Road, Dublin 12, Irlande ;
6. Exela Technologies, Vastberga Alle 36A, Hagersten, Stockholm 120 23, Suède ;
7. Exela Technologies, Eskilstunavagen 34, Strangnas 645 34, Suède ;
8. Exela Technologies, Gripengrand 4, Froson 838 80, Suède ;
9. Exela Technologies, Eskilstunavagen 34, Strangnas 645 34, Suède ;
10. Exela Technologies, Nedre Rommen 5C, Oslo 0988, Norvège ;
11. Exela Technologies, Plauener Str. 163-165, Berlin 13053, Allemagne ;
12. Exela Technologies, Hubnerstrasse 3, Augsbourg 86150, Allemagne ;
13. Exela Technologies, Monzastrasse 4c, Langen 63225, Allemagne ;
14. Exela Technologies, Grudziądzka 46-48, Toruń 87-100, Pologne ;
15. Exela Technologies, 1 Rue de la Mare Blanche, Noisiel 77186, France ;
16. Exela Technologies, 14 Rue des Landelles, Cesson Sevigne, Ille-et-Vilaine 35510, France;
17. Exela Technologies, ZAC des Foliouses, Rue de Monts d'Or, Miribel les Echets 01700, France;
18. Exela Technologies, Uraniumweg 15, 3812 RJ Amersfoort, Pays-Bas;

19. Exela Technologies, Monzastrasse 4c, Langen 63225, Allemagne.

Confidentialité, intégrité, disponibilité et résilience des systèmes et services de traitement

I.Sécurité physique et environnementale

Contrôles ISO pertinents : A.11.1.1 Périmètre de sécurité physique ; A.11.1.2 Contrôles d'entrée physique ; A.11.1.3 Sécurisation des bureaux, des pièces et des installations ; A.11.1.4 Protection contre les menaces extérieures et environnementales ; A.11.1.5 Travail dans des zones sécurisées

Exela a mis en œuvre les mesures requises, entre autres :

☒ Toutes les portes et/ou fenêtres concernées sont convenablement protégées contre les accès non autorisés par des mécanismes de contrôle (par exemple, serrures, barres, alarmes, lecteurs de badges, cartes magnétiques) ;

☒ Si nécessaire, des barrières et des périmètres supplémentaires sont mis en place pour contrôler l'accès physique entre les zones d'un même bâtiment (par exemple pour les salles de serveurs) ;

☒ L'accès aux sites et aux bâtiments est réservé au personnel autorisé ;

☒ Les droits d'accès sont accordés selon le principe du “besoin d'en connaître” et sont régulièrement révisés et mis à jour, et révoqués si nécessaire ;

☒ La date et l'heure d'entrée et de sortie des visiteurs sont enregistrées, et tous les visiteurs sont surveillés par un membre du personnel d'Exela, sauf si leur accès a été préalablement autorisé ;

☒Les équipements photographiques, vidéo, audio ou autres équipements d'enregistrement, tels que les caméras dans les appareils portables, ne sont pas autorisés, sauf si leur utilisation a été préalablement approuvée ;

☒ La protection physique contre les catastrophes naturelles, les attaques malveillantes ou les accidents est conçue et appliquée conformément aux normes nationales, régionales ou internationales.

II.Contrôles d'accès

Contrôles ISO pertinents : A.9.1.1 Politique de contrôle d'accès ; A.9.1.2 Accès aux réseaux et aux services de réseau ; A.9.2.2 Fourniture de l'accès aux utilisateurs ; A.9.2.4 Gestion des informations d'authentification secrètes des utilisateurs ; A.9.4.2 Procédures de connexion sécurisées ; A.9.4.3 Système de gestion des mots de passe ; A.12.4.1 Enregistrement des événements ; A.12.4.3 Journaux des administrateurs et des opérateurs ;

Exela a mis en œuvre les mesures requises, entre autres :

☒ La politique de contrôle d'accès est établie, documentée et revue régulièrement. Elle couvre entre autres : la séparation des rôles en matière de contrôle d'accès (par exemple, demande

d'accès), les exigences en matière d'autorisation formelle et l'examen périodique des demandes d'accès ;

☒ Des contrôles et des procédures de gestion visant à protéger l'accès aux connexions et aux services de réseau ainsi que les moyens utilisés pour accéder aux réseaux et aux services de réseau (par exemple, l'utilisation de VPN) sont en place ;

☒ Les principes du “besoin de savoir” et du “besoin d'utiliser” sont respectés ;

☒ Un processus d'attribution ou de révocation des droits d'accès accordés aux identifiants des utilisateurs est en place et comprend notamment : la garantie que les droits d'accès ne sont pas activés (par exemple par les fournisseurs de services) avant que les procédures d'autorisation ne soient terminées. En outre, Exela tient un registre central des droits d'accès accordés à un identifiant d'utilisateur pour accéder aux systèmes et services d'information ;

☒ Les informations d'authentification secrètes sont contrôlées par un processus de gestion formel ;

☒Lorsque la politique de contrôle d'accès l’exige, l'accès aux systèmes et aux applications est contrôlé par une procédure de connexion sécurisée ;

☒Les systèmes de gestion de mots de passes sont interactifs et garantissent la qualité des mots de passe (par exemple, les utilisateurs sont obligés de changer leur mot de passe à intervalles réguliers et nous suivons une règle qui consiste à ne pas afficher les mots de passe à l'écran lors de la saisie).

☒Les journaux de bord enregistrant les activités des utilisateurs, les exceptions, les défauts et les événements liés à la sécurité de l'information sont conservés et régulièrement révisés.

III. Gestion des actifs et des données

Contrôles ISO pertinents : A.8.1.1 Inventaire des actifs ; A.8.2.1 Classification des informations ; A.8.2.2 Étiquetage des informations ; A.8.3.1 Gestion des supports amovibles ; A.12.2.1 Contrôles contre les logiciels malveillants ; A.12.3.1 Sauvegarde des informations ;

Exela a mis en œuvre les mesures requises, entre autres :

☒ Exela a identifié les actifs et leurs propriétaires dans le cycle de vie des informations, a documenté leur importance et a créé un inventaire de ces actifs qui est régulièrement tenu à jour ;

☒ Les classifications et les contrôles de protection des informations qui y sont associés comprennent les besoins des entreprises en matière de partage ou de restriction des informations, ainsi que les exigences légales. Le niveau de protection du système est évalué en analysant la confidentialité, l'intégrité et la disponibilité ainsi que toute autre exigence relative aux informations considérées. Les propriétaires des actifs d'information sont responsables de leur classification ;

☒ Un ensemble approprié de procédures pour l'étiquetage des informations est élaboré et mis en œuvre conformément au système de classification des informations adopté au sein d'Exela. Les employés sont informés des procédures d'étiquetage ;

☒ Les procédures de gestion des supports amovibles conformément au système de classification sont mises en œuvre (par exemple, tous les supports sont stockés dans un environnement sûr et sécurisé, conformément aux spécifications des fabricants) ;

☒ Des contrôles de détection, de prévention et de récupération visant à protéger contre les logiciels malveillants sont mis en œuvre, associés à une sensibilisation appropriée des utilisateurs ;

☒ Des copies de sauvegarde des informations, des logiciels et des images du système sont régulièrement testées conformément à une politique de sauvegarde convenue ;

☒ Les sauvegardes sont stockées dans un endroit éloigné, à une distance suffisante pour éviter tout dommage lors d'une catastrophe sur le site principal.

IV. Communication

Contrôles ISO pertinents : A.13.1.1 Contrôles des réseaux ; A.13.1.3 Séparation dans les réseaux ; A.13.2.2 Accords sur le transfert d'informations ; A.13.2.4 Accords de confidentialité ou de non-divulgation

Exela a mis en œuvre les mesures requises, entre autres :

☒ Les réseaux sont gérés et contrôlés pour protéger les données dans les systèmes et les applications (par exemple, la connexion des systèmes au réseau est restreinte et authentifiée, des contrôles spéciaux sont établis pour sauvegarder la confidentialité et l'intégrité des données) ;

☒ Les groupes de services d'information, d'utilisateurs et de systèmes d'information sont séparés sur les réseaux. L'accès est contrôlé au niveau du périmètre par une passerelle (par exemple un pare-feu) ;

☒ Des accords de transfert sont en place ;

☒ Les accords de non-divulgation reflétant les besoins d'Exela en matière de protection sont identifiés, régulièrement révisés et documentés.

V.Conformité

Contrôles ISO pertinents : A.18.1.1 Identification de la législation applicable et des exigences contractuelles ; A.18.1.3 Protection des dossiers ; A.18.1.4 Vie privée et protection des informations personnelles identifiables

Exela a mis en œuvre les mesures requises, entre autres :

☒ Toutes les exigences législatives, réglementaires et contractuelles pertinentes sont identifiées, documentées et mises à jour. Les contrôles spécifiques et les responsabilités individuelles à respecter sont également définis et documentés ;

☒ Toutes les données sont protégées contre la perte, la destruction, la falsification, l'accès non autorisé et la diffusion non autorisée, conformément aux exigences législatives, réglementaires, contractuelles et commerciales ;

☒ La vie privée et la protection des données personnelles sont assurées comme l'exigent la législation et la réglementation applicables, notamment le RGPD et le RU-RGPD.

La capacité de rétablir la disponibilité et l'accès aux données personnelles en temps utile en cas d'incident physique ou technique

I. Gestion des incidents

Contrôles ISO pertinents : A.16.1.2 Signalement des événements de sécurité de l'information ; A.16.1.3 Signalement des faiblesses de la sécurité de l'information ; A.16.1.4 Évaluation des événements de sécurité de l'information et décision à leur sujet ; A.16.1.5 Réponse aux incidents de sécurité de l'information ; A.16.1.7 Collecte de preuves

Exela a mis en œuvre les mesures requises, entre autres :

☒ Les procédures et processus pertinents pour assurer une réponse rapide, efficace et ordonnée aux incidents de sécurité de l'information sont mis en œuvre et régulièrement révisés. La classification et la hiérarchisation des incidents sont définies ;

☒ Tous les employés sont au courant de leur responsabilité de signaler les incidents de sécurité de l'information ainsi que de l'existence de procédures de signalement et du point de contact auquel les événements doivent être signalés ;

☒ La collecte, l'acquisition et la conservation des preuves, en fonction des différents types de supports, de dispositifs et de l'état des dispositifs sont définis.

II. Gestion de la continuité

Contrôles ISO pertinents : A.12.3.1 Sauvegarde des informations ; A.17.1.1 Planification de la continuité de la sécurité des informations ; A.17.1.2 Mise en œuvre de la continuité de la sécurité des informations ; A.17.2.1 Disponibilité des installations de traitement des informations.

Exela a mis en œuvre les mesures requises, entre autres :

☒ Les exigences en matière de sécurité de l'information et de continuité de la gestion de la sécurité de l'information dans des situations défavorables (par exemple, lors d'une crise ou d'une catastrophe) ont été définies ;

☒ Les processus, procédures et contrôles sont établis, documentés, mis en œuvre et maintenus pour assurer le niveau de continuité requis pour la sécurité des informations en cas de situation défavorable ;

☒ La continuité de la gestion de la sécurité de l'information est vérifiée, entre autres, en exerçant et en testant la fonctionnalité des processus, procédures et contrôles de continuité de la sécurité de l'information afin de s'assurer qu'ils sont conformes aux objectifs de continuité de la sécurité de l'information ;

☒ Le cas échéant, les systèmes d'information redondants doivent être testés pour s'assurer que le basculement d'un composant à l'autre fonctionne comme prévu ;

☒ Les supports de sauvegarde sont régulièrement testés afin de s'assurer qu'ils peuvent être utilisés en cas d'urgence lorsque cela est nécessaire.

Évaluer et apprécier l'efficacité des mesures techniques et organisationnelles

I. Examens

Contrôles ISO pertinents : A.18.2.1 Examen indépendant de la sécurité de l'information ; A.18.2.2 Respect des politiques et des normes de sécurité ; A.18.2.3 Examen de la conformité technique

Exela a mis en œuvre les mesures requises, entre autres :

☒ Les contrôles, objectifs, politiques, processus et procédures font l'objet d'un examen indépendant à intervalles planifiés et/ou lorsque des changements importants surviennent.

☒ Nous menons des actions supplémentaires en cas de non-respect des règles (par exemple, identifier les causes du non-respect, évaluer la nécessité d'actions pour parvenir à la conformité, mettre en œuvre des mesures correctives appropriées, examiner les mesures correctives prises pour vérifier leur efficacité et identifier les lacunes ou les faiblesses) ;

☒ Les examens de conformité technique impliquent l'examen des systèmes opérationnels pour s'assurer que les contrôles du matériel et des logiciels ont été correctement mis en œuvre.

Pseudonymisation et cryptage des données personnelles

Contrôles ISO pertinents :

A.10.1.1 Politique relative à l'utilisation des contrôles cryptographiques ; A.10.1.2 Gestion des clés ; A.14.3.1 Protection des données d'essai ; A.18.1.5 Réglementation des contrôles cryptographiques

Exela a mis en œuvre les mesures requises, entre autres :

☒ Une politique sur l'utilisation de contrôles cryptographiques pour la protection des informations est élaborée et mise en œuvre ;

☒ Sur la base d'une évaluation des risques, le niveau de protection requis est déterminé en tenant compte du type, de la puissance et de la qualité de l'algorithme de cryptage requis ;

☒ Une politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques est élaborée et mise en œuvre. Les algorithmes cryptographiques, la longueur des clés et les pratiques d'utilisation sont sélectionnés en fonction des meilleures pratiques ;

☒ Toutes les clés cryptographiques doivent être protégées contre la modification et la perte. En outre, les clés secrètes et privées doivent être protégées contre l'utilisation et la divulgation

non autorisées. Les équipements utilisés pour générer, stocker et archiver les clés sont physiquement protégés ;

☒ Toute donnée de test est sélectionnée avec soin, protégée et contrôlée ;

☒ Les contrôles cryptographiques sont conformes à tous les accords, lois et règlements pertinents.