Groupe BASF –
Addendum sur la cybersécurité

Version **5.1**

Classification **P U B L I C**

Détails de la version

Version	5.1
Créé par	Sebastian Krüsmann, NeoMINT GmbH
Statut	Approuvé

Approuvé le	10.01.2024
Approuvé par	Julia Mansky, BASF Digital Solutions GmbH
Mises à jour sur	Centre de téléchargement (basf.com)

Historique des modifications

Version	Date	Créée par	Changements
1.0	02.10.2023	Sebastian Krüsmann, NeoMINT GmbH	Création initiale
2.0	09.10.2023	Sebastian Krüsmann, NeoMINT GmbH	Modifications rédactionnelles
3.0	17.10.2023	Sebastian Krüsmann, NeoMINT GmbH	Modifications rédactionnelles
4.0	21.11.2023	Sebastian Krüsmann, NeoMINT GmbH	Modifications rédactionnelles
5.0	08.01.2024	Sebastian Krüsmann, NeoMINT GmbH	Modifications rédactionnelles
5.1	08.08.2024	Beatrice Huck, NeoMint Gmbh	Ajout des commandes C-T-12 et S-T-12, CL-T-15 Changement de contrôle C-T-13, S-T-13, CL-T-16, CL-T-09, C-T-06 et S-T-06

Table des matières

1 Note préliminaire

L'addendum sur la sécurité contient des exigences en matière de sécurité de l'information.

Tous les fournisseurs informatiques sont tenus de respecter les spécifications du chapitre « **Général** ». Les autres exigences sont classées en fonction du type de services fournis et doivent être remplies en conséquence. Vous trouverez une description des services au début de chaque chapitre.

Pour chaque type de service fourni / de fournisseur, un chapitre décrit les risques spécifiques et la situation sans risque qu'il faut atteindre. À cette fin, il existe diverses mesures de nature technique ou organisationnelle qui peuvent généralement être appliquées. Si le risque n'est pas pertinent pour un cas particulier ou si un fournisseur est d'avis qu'un risque pourrait être évité d'une manière différente de celle indiquée, il est possible de l'expliquer brièvement. Il appartient à BASF de décider si les raisons et les mesures données sont suffisantes.

2 Interlocuteurs pour la cybersécurité

Afin d'assurer une coopération transparente et efficace avec nos fournisseurs informatiques dans le but de maintenir un niveau approprié de cybersécurité, chaque fournisseur doit donner les noms et les coordonnées des personnes en charge des rôles de base en matière de cybersécurité.

Pour chaque fournisseur, les informations sont documentées par le client interne (iBP ou achats) dans le formulaire *2 Fiche de Assessment_EN_Contact de sécurité des fournisseurs informatiques* dans la version actuelle en allemand ou en anglais et envoyées à l'équipe de sécurité des fournisseurs.

3 Généralités

La section sécurité générale des fournisseurs est pertinente si des risques existent, quel que soit le service fourni.

3.1 Point de contact (SPoC) unique pour la cybersécurité / la sécurité de l'information

Risque visé : Une communication inadéquate ou tardive avec les fournisseurs sur les questions de cybersécurité pourrait entraîner le traitement tardif ou inadéquat des vulnérabilités.

Objectif : Les questions sur des problèmes de cybersécurité, par exemple sur les mesures de sécurité mises en œuvre ou en cas de découverte d'incidents de sécurité affectant le fournisseur, recevront une réponse dans un délai raisonnable.

Mesures techniques

G-T-01	Plate-forme par laquelle les demandes sont soumises et répondues rapidement, par exemple système de tickets

Mesures organisationnelles

G-O-01	Interlocuteur dédié pour les questions de cybersécurité, par exemple, RSSI / responsable de la sécurité de l'information

3.2 Sécurité des ressources humaines

Risque visé : Les employés des fournisseurs pourraient avoir un impact négatif significatif sur le niveau de sécurité de BASF par leur comportement, à la fois intentionnel et par négligence.
Objectif Seuls les employés suffisamment qualifiés et informés ont accès aux informations ou aux systèmes de BASF.

Mesures techniques

G-T-02	Concept de rôle et d'autorisation : Les employés n'ont accès qu'aux renseignements pertinents pour leur travail (principe du besoin de savoir)

Mesure organisationnelle

G-O-02 Des formations régulières de sensibilisation sur les thèmes de la cybersécurité pour tous les collaborateurs

3.3 Gestion de la sécurité de l'information

Risque visé : Une conceptualisation et un plan d'opérations insuffisants de la cybersécurité pourraient faire en sorte que les vulnérabilités ne soient pas identifiées ou évitées à un stade précoce. L'exploitation de telles vulnérabilités par un attaquant pourrait avoir un impact négatif sur le niveau de sécurité de BASF.

Objectif : Conception et gestion proactive de l'ensemble des mécanismes de sécurité du fournisseur.

Mesures organisationnelles

G-O-03 Nomination d'une personne responsable du maintien d'un niveau approprié de cybersécurité, p. ex., chef de la sécurité de l'information ou agent de sécurité de l'information

G-O-04 Gestion de l'ensemble des mesures de cybersécurité dans le cadre d'un système de management de la sécurité de l'information (SMSI)

G-O-05 Certification du système de gestion de la sécurité de l'information sur la base d'une norme établie, e.g. ISO 27001

3.4 Sécurité de la chaîne d'approvisionnement

Risque visé : Une conceptualisation et une opérationnalisation insuffisantes de la cybersécurité pourraient faire en sorte que les vulnérabilités ne soient pas identifiées ou évitées à un stade précoce. L'exploitation de telles vulnérabilités par un attaquant pourrait avoir un impact négatif sur le niveau de sécurité de BASF.

Objectif : Exiger de la part de tous les sous-traitants et fournisseurs qu'ils établissent et maintiennent un niveau approprié de cybersécurité.

Mesures organisationnelles

G-O-06 Référencement des sous-traitants engagés pour la fourniture de services à BASF

G-O-07 Obligation contractuelle donnée aux sous-traitants et aux fournisseurs d'établir et de maintenir un niveau approprié de cybersécurité

3.5 Gestion du changement

Risque visé : Un contrôle inapproprié des modifications apportées aux services et produits fournis pourrait entraîner des pertes d'information et une dégradation des performances, ce qui pourrait avoir un impact négatif sur les activités de BASF.

Objectif : Établir une procédure normalisée et formalisée pour coordonner et suivre l'application des changements concernant les services et produits fournis.

Mesures techniques

G-T-03 Plateforme par laquelle toutes les modifications de contrats et de services sont gérées et documentées

Mesures organisationnelles

G-O-08 (Simple) Point de contact (SPoC) pour les modifications des services contractés

3.6 Conformité

Risque visé : BASF pourrait être tenu responsable des infractions légales et réglementaires commises par les fournisseurs.

Objectif : Toutes les exigences de conformité applicables sont à tous moments respectés.

Mesures organisationnelles

G-O-09 Nomination d'une personne responsable du maintien de la conformité à l'échelle mondiale, p. ex. agent de conformité

G-O-10 Gestion de toutes les mesures de conformité dans le cadre d'un système de gestion de la conformité (CMS)

4 Services de consulting

Description : Tous les services de consulting qui sont liés de près ou de loin à la gestion de projet, ainsi qu'à la fourniture, à l'exploitation ou à la mise hors service de solutions informatiques.

4.1 Gestion des ressources

Risque visé : Les pénuries de personnel pourraient entraîner la non-fourniture de services convenus contractuellement.

Objectif : Garantir à tout moment que des employés suffisamment qualifiés sont disponibles pour la fourniture des services convenus contractuellement. Tous les services peuvent être livrés à temps et dans la qualité convenue.

Mesures organisationnelles

C-O-01 Gestion des ressources humaines dans le cadre de la gestion des ressources internes afin de fournir du personnel qualifié

C-O-02 Concept de formation et de développement pour le personnel spécialisé et les cadres

4.2 Traitement de l'information

Risque visé : Les informations utilisées dans le cadre de projets de conseil pourraient compromettre la cybersécurité de BASF en cas de perte de confidentialité.

Objectif : Garantir à tout moment que toutes les informations créées et reçues dans le cadre des projets de conseil sont traitées de manière confidentielle et protégées contre toute compromission.

Mesures techniques

C-T-01 Cryptage des communications par courrier électronique à l'aide d'une norme industrielle établie, p. ex. PGP, S/MIME

C-T-02 Cryptage des disques durs d'appareils mobiles, par exemple BitLocker, Vera Crypt

Réf. C-T-03	Cryptage des disques durs des serveurs, par exemple BitLocker, Vera Crypt
C-T-04	Cryptage des supports de données mobiles, par exemple BitLocker, Vera Crypt, cryptage du matériel
C-T-05	Gestion de toutes les autorisations dans le cadre de la gestion des identités et des accès (IAM) de bout en bout

Mesures organisationnelles

C-O-03	Procédure de stockage, de traitement et d'envoi des informations avant, pendant et après les projets
C-O-04	Processus de traitement des incidents en matière de sécurité
C-O-05	Processus d'effacement à distance des données en cas de perte d'appareils mobiles
C-O-06	Processus visant à s'assurer que seuls les employés qui fournissent des services de conseil à BASF ont accès à l'information de BASF (principe du besoin de savoir)
C-O-07	Processus pour l'octroi, la modification ou la révocation des droits d'accès lorsque les employés rejoignent l'entreprise, la quittent ou changent de poste (processus Joiner-Mover-Leaver)
C-O-08	Concept de classification des informations traitées en fonction de leur criticité

4.3 Protection contre les logiciels malveillants

Risque visé : si les appareils informatiques utilisés dans le processus de conseil sont compromis, des informations pourraient être modifiées par inadvertance ou rendues accessibles par des tiers non autorisés.

Objectif : Garantir qu'aucun logiciel malveillant ne peut être installé sur les appareils informatiques.

Mesures techniques

C-T-06 Solution de protection contre les logiciels malveillants pour les serveurs Windows

C-T-07 Solution de protection contre les logiciels malveillants sur les clients, par exemple Microsoft Defender

Réf. C-T-08 Appareils de sécurité, par ex. Pare-feu, SIEM

C-T-09 Segmentation appropriée du réseau de l'entreprise en fonction de la criticité en matière de confidentialité et de disponibilité des données traitées

C-T-10 Utilisation d'une solution de bac à sable pour ouvrir des fichiers inconnus ou des fichiers provenant d'expéditeurs inconnus.

C-T-11 Distribution des logiciels gérée de manière centralisée

C-T-12 Interdiction d'accorder des droits d'administration locale aux développeurs d'applications

C-T-13 Interdiction d'accorder des droits d'administration locale aux utilisateurs réguliers

Mesures organisationnelles

C-O-09 Processus d'installation immédiate des mises à jour des logiciels quand elles concernent la sécurité

C-O-10 Durcir les procédures de sécurité des serveurs

C-O-11 Durcir les procédures de sécurité pour les clients

C-O-12 Durcir les procédures de sécurité pour les smartphones

4.4 Sauvegarde des données

Risque visé : les erreurs système, les logiciels malveillants ou une mauvaise utilisation des systèmes informatiques peuvent entraîner la perte des données collectées dans le cadre d'un projet de conseil.

Objectif : Toutes les données pertinentes pour BASF sont sauvegardées régulièrement et peuvent être restaurées en cas de perte.

Mesures techniques

C-T-14 Sauvegardes régulières et automatisées de toutes les données pertinentes pour BASF

Mesures organisationnelles

C-O-13 Concept de sauvegarde des données

C-O-14 Exercices réguliers de sauvegarde et de récupération de données

4.5 Sécurité physique

Risque visé : Lorsqu'elles sont traitées dans les locaux d'un fournisseur, les informations BASF peuvent être compromises par des parties externes.

Objectif : Toutes les informations provenant de BASF et concernant BASF sont protégées contre tout accès physique par des tiers non autorisés.

Mesures techniques

C-T-15 Bureaux verrouillables

C-T-16 Armoires verrouillables ou coffres-forts

Mesures organisationnelles

C-O-15 Procédure pour que le fournisseur fasse accompagner ses visiteurs par son personnel

C-O-16 Procédure de verrouillage des supports de stockage de données, des équipements et des documents informatiques

4.6 Protection des informations personnelles identifiables (PII)

Risque visé : Lors du traitement d'informations personnelles dans le cadre d'un contrat, les droits des personnes concernées peuvent être compromis par une utilisation inappropriée des informations.

Objectif : Lors du traitement des données personnelles, il est garanti à tout moment que les exigences du RGPD et des réglementations en aval sur la protection des données sont respectées.

Mesures organisationnelles

C-O-17 Nomination d'une personne responsable de la protection des données, par exemple un délégué à la protection des données

C-O-18 Protection de l'ensemble des informations personnelles identifiables dans le cadre d'un système de gestion de la protection des données (DMS)

5 Service et assistance

Description : Tous les services, dont l'assistance, dans le cadre desquels des solutions IT sont administrées, entretenues ou supprimées. Cela couvre l'ensemble du cycle de vie d'une solution et commence par l'installation et se termine par l'élimination.

5.1 Gestion des ressources

Risque visé : Le manque de personnel pourrait entraîner la non-fourniture de services convenus contractuellement.

Objectif : Garantir à tout moment que des employés suffisamment qualifiés sont disponibles pour la fourniture des services prévus dans le contrat. Tous les services peuvent être fournis à temps et avec la qualité convenue.

Mesures organisationnelles

S-O-01 Gestion des ressources humaines dans le cadre de la gestion des ressources internes afin de fournir du personnel qualifié

N° S-O-02 Concept de formation et de développement pour le personnel spécialisé et les manageurs

5.2 Traitement de l'information

Risque visé : Les informations utilisées dans le cadre des services fournis et des missions d'assistance pourraient compromettre la cybersécurité de BASF en cas de perte de confidentialité.

Objectif : Garantir à tout moment que toutes les informations créées et reçues dans le cadre des services fournis sont traitées de manière confidentielle et protégées contre tout dommage.

Mesures techniques

S-T-01 Cryptage des communications par courrier électronique à l'aide d'une norme industrielle établie, par exemple PGP, S/MIME

S-T-02 Cryptage des disques durs d'appareils mobiles, par exemple BitLocker, Vera Crypt

S-T-03 Cryptage des disques durs des serveurs, par exemple BitLocker, Vera Crypt

S-T-04	Cryptage des supports de données mobiles, par exemple BitLocker, Vera Crypt, cryptage du matériel

S-T-05	Gestion de toutes les autorisations dans le cadre de la gestion des identités et des accès (IAM) de bout en bout

Mesures organisationnelles

S-O-03	Procédure de stockage, de traitement et d'envoi des informations avant, pendant et après les missions

N° S-O-04 Processus de traitement des incidents en matière de sécurité

S-O-05 Processus d'effacement à distance des données en cas de perte d'appareils mobiles

S-O-06	Processus visant à s'assurer que seuls les employés qui fournissent des services de conseil à BASF ont accès à l'information de BASF (principe du besoin de savoir)

S-O-07	Processus pour l'octroi, la modification ou la révocation des droits d'accès lorsque les employés rejoignent ou quittent l'entreprise ou changent de poste (processus Joiner-Mover-Leaver)

Réf. S-O-08 Concept de classification des informations traitées en fonction de leur criticité

5.3 Protection contre les logiciels malveillants

Risque visé : Si les appareils informatiques utilisés dans le cadre des missions de services et d'assistance sont compromis, des informations peuvent être modifiées par inadvertance ou rendues accessibles à des tiers non autorisés.

Objectif : Garantir qu'aucun logiciel malveillant ne peut être installé sur les appareils informatiques.

Mesures techniques

S-T-06 Solution de protection contre les logiciels malveillants pour les serveurs Windows

S-T-07 Solution de protection contre les logiciels malveillants sur les clients, par exemple Microsoft Defender

S-T-08 Appareils de sécurité, par ex. Pare-feu, SIEM

S-T-09 Segmentation appropriée du réseau de l'entreprise en fonction de la criticité en matière de confidentialité et de disponibilité des données traitées

S-T-10 Utilisation d'une solution de bac à sable pour ouvrir des fichiers inconnus ou des fichiers provenant d'expéditeurs inconnus.

S-T-11 Distribution des logiciels gérée de manière centralisée

S-T-12 Interdiction d'accorder des droits d'administrateur aux développeurs

S-T-13 Interdiction d'accorder des droits d'administrateur aux utilisateurs

Mesures organisationnelles

S-O-09 Processus d'installation immédiate des mises à jour des logiciels quand elles concernent la sécurité

S-O-10 Durcir les procédures de sécurité des serveurs

S-O-11 Durcir les procédures de sécurité pour les clients

S-O-12 Durcir les procédures de sécurité pour les smartphones

5.4 Sauvegarde des données

Risque visé : Les erreurs systèmes, les logiciels malveillants ou l'utilisation abusive des systèmes informatiques peuvent entraîner la perte de données pertinentes pour BASF.

Objectif : Toutes les données pertinentes pour BASF sont sauvegardées régulièrement et peuvent être restaurées en cas de perte.

Mesures techniques

S-T-14 Sauvegardes régulières et automatisées de toutes les données pertinentes pour BASF

Mesures organisationnelles

S-O-13 Concept de sauvegarde des données

S-O-14 Exercices réguliers de sauvegarde et de récupération des données

5.5 Sécurité physique

Risque visé : Lorsqu'elles sont traitées dans les locaux d'un fournisseur, les informations de BASF peuvent être compromises par des tiers externes.

Objectif : Toutes les informations provenant de BASF et concernant BASF sont protégées contre tout accès physique par des tiers non autorisés.

Mesures techniques

S-T-15 Bureaux verrouillables

S-T-16 Armoires verrouillables ou coffres-forts

Mesures organisationnelles

S-O-15 Procédure pour que le fournisseur fasse accompagner ses visiteurs par son personnel

S-O-16 Procédure de verrouillage des supports de stockage de données, des équipements et des documents informatiques

5.6 Protection des informations personnelles identifiables (PII)

Risque visé : Lors du traitement d'informations personnelles dans le cadre du contrat, les droits de certaines personnes peuvent être compromis par une utilisation inappropriée des informations.

Objectif : Lors du traitement des données personnelles, il est garanti à tout moment que les exigences du RGPD et des réglementations en aval sur la protection des données sont respectées.

Mesures organisationnelles

S-O-17 Nomination d'une personne responsable de la protection des données, par exemple un délégué à la protection des données

S-O-18 Protection de l'ensemble des informations personnelles identifiables dans le cadre d'un système de gestion de la protection des données (DMS)

5.7 Accès à distance

Risque visé : Des sessions d'accès à distance pourraient être utilisées par des personnes non autorisées comme passerelle vers le réseau BASF. Des protocoles, des configurations, des mots de passe et des applications non sécurisés peuvent permettre un accès non autorisé.

Objectif : Lors de tout accès à distance, la protection des informations et des données stockées, traitées et transmises ainsi que l'intégrité de l'infrastructure BASF sont assurées.

Mesures techniques

S-T-17 Utilisation de protocoles sécurisés, de méthodes de cryptage et d'applications lors de l'accès aux données et à l'infrastructure de BASF

Mesures organisationnelles

S-O-19 Documentation complète ou enregistrement de toutes les sessions d'accès à distance

5.8 Administration informatique

Risque visé : Une mauvaise administration informatique peut entraîner une perturbation ou compromettre l'infrastructure de BASF.

Objectif : Toutes les activités de service et d'assistance sont exécutées conformément aux meilleures pratiques de l'industrie en matière d'administration sécurisée.

Mesures techniques

S-T-18 Système de tickets pour la gestion des demandes de service et d'assistance

Mesures organisationnelles

S-O-20 Gestion et documentation des outils utilisés par le personnel au service de BASF

S-O-21 Installation immédiate des mises à jour et des correctifs des logiciels quand ils concernent la sécurité

S-O-22 Processus décrivant les services fournis disponible.

6 Matériel

Description : Achat de matériel individuel qui est installé dans les terminaux ou pour l'utilisation duquel un port de connexion est nécessaire, par exemple souris, clavier, écran, RAM, disques durs, etc.

6.1 Livraison

Risque visé : Le matériels peut être endommagé pendant la livraison. De plus, il peut être manipulé pour compromettre l'infrastructure de BASF.

Objectif : Tout le matériel livré est entièrement fonctionnel et dans la configuration prévue.

Mesures techniques

H-T-01 Plateforme de réception, de traitement et de résolution des réclamations et des retours

H-O-01 Processus pour s'assurer que chaque expédition est complète avant l'envoi

Mesures organisationnelles

H-O-02 Suivi des expéditions en temps réel

H-O-03 Protection des envois contre tout dommage

H-O-04 Scellement de tous les envois

6.2 Sécurité des produits

Risque visé : Des composants inadaptés, endommagés ou manipulés peuvent entraîner des perturbations ou compromettre l'infrastructure de BASF.

Objectif : Tous les composants matériels sont testés en termes de fonctionnalité et d'intégrité par le fournisseur ou un fournisseur en amont. Une documentation technique suffisante est disponible pour tous les composants matériels afin de sélectionner les composants optimaux pour une application donnée.

Mesures organisationnelles

H-O-05 Documentation de l'environnement de fonctionnement idéal pour tous les composants

H-O-06 Processus de validation de la fonctionnalité et de l'intégrité de tous les composants par le fournisseur ou un fournisseur en amont.

7 Terminaux et appareils

Description : Achat d'appareils destinés à être utilisés par les utilisateurs finaux ou dans un datacenter, par exemple des ordinateurs portables, des smartphones, des serveurs, etc., ainsi que d'appareils à usage unique ou dotés de systèmes d'exploitation spécialisés qui sont essentiels au fonctionnement, tels que des pares-feux, des passerelles VPN, des routeurs ou des commutateurs.

7.1 Livraison

Risque visé : Les appareils peuvent être endommagés pendant la livraison. De plus, des composants pourraient être manipulés pour compromettre l'infrastructure de BASF.

Objectif : Toutes les preuves sont fournies que les matériels livrés sont entièrement fonctionnels et dans la configuration prévue.

Mesures techniques
E-T-01 Plateforme de réception, de traitement et de résolution des réclamations et des retours

Mesures organisationnelles
E-O-01 Processus pour s'assurer de l'exhaustivité de chaque livraison avant l'expédition
E-O-02 Suivi des expéditions en temps réel
E-O-03 Protection des envois contre tout dommage
E-O-04 Scellement de tous les envois

7.2 Sécurité du produit

Risque visé : Des appareils inadaptés, endommagés ou manipulés peuvent entraîner des perturbations ou une compromission de l'infrastructure de BASF.

Objectif : Tous les appareils sont testés en termes de fonctionnalité et d'intégrité par le fournisseur ou un fournisseur en amont. Une documentation technique suffisante est disponible

pour tous les composants afin de sélectionner les composants optimaux pour une application donnée.

Mesures organisationnelles

E-O-05	Documentation de l'environnement de fonctionnement idéal pour tous les composants
E-O-06	Processus de validation de la fonctionnalité et de l'intégrité de tous les composants par le fournisseur ou un fournisseur en amont

7.3 Configuration de l'appareil

Risque visé : Quand les appareils sont initialement configurés par le fournisseur, l'utilisation de configurations par défaut courantes et donc facilement prévisibles peut permettre aux attaquants de compromettre BASF.

Objectif : Les mises à jour et les correctifs liés à la sécurité disponibles au moment de l'installation sont installés sur tous les appareils. Les mots de passe initiaux sont configurés de manière à être modifiés par l'utilisateur lors de la première connexion.

Mesures organisationnelles

E-O-07	Installation de toutes les mises à jour et correctifs disponibles pour le système d'exploitation et le firmware
E-O-08	Utilisation de mots de passe initiaux qui doivent être modifiés lors de la première utilisation de l'appareil
E-O-09	Éviter l'installation de progiciels qui ne sont pas indispensables, par exemple les logiciels OEM optionnels

8 Solutions Locales

Explication : Achat d'applications (packages) qui sont exécutées dans l'infrastructure BASF (par exemple sur des ordinateurs portables, des serveurs ou des smartphones) et qui ne nécessitent pas d'accès aux systèmes du fabricant pour être utilisées.

8.1 Concept de sécurité informatique

Risque visé : Si les mécanismes de sécurité standard de l'industrie ne sont pas pris en compte lors de la planification et du développement, ou si les interactions entre les mesures prises (techniques ou organisationnelles) ne sont pas reconnues, les attaquants pourraient exploiter les vulnérabilités de sécurité qui en résultent et compromettre les informations, les données et l'infrastructure de BASF.

Objectif : L'ensemble des mesures de sécurité d'une solution sont définies dans le cadre d'un concept de sécurité informatique. Le suivi de l'implémentation est documenté et mis à jour en permanence lorsque des modifications sont apportées.

Mesures organisationnelles

O-O-01 Développement d'un concept de sécurité informatique pour la solution

---

O-O-02 Mise à jour régulière du concept de sécurité informatique ainsi qu'en cas de modifications

---

O-O-03 Fourniture à BASF de la documentation sur les mécanismes de sécurité mis en œuvre

8.2 Cryptographie

Risque visé : Si les données ne sont pas protégées pendant le stockage, le traitement ou la transmission, elles pourraient être interceptées ou compromises par des tiers non autorisés.

Objectif : Tout au long du cycle de vie, les données sont protégées contre tout accès non autorisé.

Mesures techniques

O-T-01 Cryptage des données lors du transfert (Data at Transit), par exemple HTTPS, SSH

O-T-02 Cryptage des données pendant le stockage, par exemple cryptage de la base de données

O-T-03 Authentification multi facteurs pour l'accès aux informations sensibles

O-T-04 Authentification multi facteurs pour les modifications de configuration

Mesures organisationnelles

O-O-04 Concept de cryptographie avec toutes les méthodes de cryptage mises en œuvre et les longueurs de clé

8.3 Concept en matière de rôles et d'autorisations

Risque visé : Un concept en matière de rôles et d'autorisations manquant ou incorrect pourrait permettre à des utilisateurs non autorisés d'accéder à des informations sensibles.

Objectif : Les rôles et les autorisations peuvent être gérés de manière granulaire afin que les utilisateurs n'aient accès qu'aux informations dont ils ont besoin pour effectuer leurs tâches.

Mesures techniques

O-T-05 Active Directory API

O-T-06 LDAP API

O-T-07 Attribution d'autorisations exclusivement via l'attribution de rôles

O-T-08 Module logiciel / composant / fonction pour la gestion des rôles et des autorisations

Mesures organisationnelles

O-O-05 Concept formalisé et documenté de rôles et d'autorisations

8.4 Mises à jour et correctifs

Risque visé : Si les mises à jour et les correctifs de sécurité ne sont pas installés immédiatement après leur publication, les attaquants pourraient reconstruire et exploiter la vulnérabilité corrigée par la mise à jour ou le correctif.

Objectif : Le délai entre la publication des mises à jour et des correctifs, leur mise à disposition chez BASF et leur installation est si court qu'il est impossible pour les attaquants d'exploiter les vulnérabilités connues.

Mesures techniques

O-T-09 Mise à disposition de mises à jour et de correctifs liés à la sécurité au sein de la solution

---

O-T-10 Mise à disposition de mises à jour et de correctifs liés à la sécurité via le site web du fournisseur

Mesures organisationnelles

O-O-06 Information par email sur les mises à jour et les correctifs récemment publiés

---

O-O-07 Informations sur les mises à jour et les correctifs récemment publiés dans la solution elle-même

---

O-O-08 Information via le site Web du fournisseur sur les mises à jour et les correctifs récemment publiés

8.5 Tests d'intrusion

Risque visé : La complexité des solutions peut faire que les vulnérabilités passent inaperçues du fait de l'interaction des sous-composants et des effets qui en résultent. Ces angles morts pourraient être exploités par les attaquants.

Objectif : Le niveau de protection de l'ensemble de la solution est régulièrement réexaminé en tenant compte de toutes les méthodes d'attaques connues. En fonction des résultats, le niveau de protection sera redéveloppé.

Mesures organisationnelles

O-O-09	Des tests d'intrusion réguliers de la solution
O-O-10	Tests d'intrusion de la solution mis en place lors d'événements, par exemple en cas de modifications importantes
O-O-11	Tests d'intrusion réguliers de composants tiers, par exemple des modules logiciels de développeurs externes
O-O-12	Tests d'intrusion de composants tiers mis en place lors d'événements, par exemple lorsque des vulnérabilités ou des incidents de sécurité sont identifiés

8.6 Support et documentation pour les utilisateurs

Risque visé : Des instructions utilisateur manquantes ou indisponibles peuvent entraîner une non-utilisation ou une utilisation incorrecte de la solution. Cela pourrait avoir un effet négatif sur les activités de BASF.

Objectif : Tous les groupes d'utilisateurs sont autorisés à utiliser la solution de la manière prévue et pour l'usage prévu.

Mesures techniques

O-T-11	Forum communautaire d'échange entre utilisateurs
O-T-12	Site web d'assistance pour les utilisateurs
O-T-13	Hotline téléphonique pour les utilisateurs

O-T-14 Assistance par e-mail pour les utilisateurs

Mesures organisationnelles

O-O-13 Formations proposées aux utilisateurs par les formateurs du fournisseur

O-O-14 Formations proposées aux utilisateurs par des prestataires externes, par exemple des associations industrielles, TÜV (Association allemande de contrôle technique)

O-O-15 Matériel d'auto-apprentissage pour l'utilisateur, par exemple vidéos tutoriels, présentations, instructions étape par étape

O-O-16 Manuels d'utilisation

O-O-17 Manuels d'utilisation basés sur des scénarios

8.7 Support et documentation pour les administrateurs

Risque visé : Une installation, une distribution ou une configuration incorrecte peuvent entraîner la compromission des données ou la défaillance de la solution, perturbant ainsi l'activité de BASF.

Objectif : Les administrateurs BASF responsables de l'exploitation de la solution sont habilités à gérer la solution comme prévu.

Mesures techniques

O-T-15 Forum communautaire d'échange entre administrateurs

O-T-16 Site web d'assistance pour les administrateurs

O-T-17 Hotline téléphonique pour les administrateurs

O-T-18 Assistance par e-mail pour les administrateurs

Mesures organisationnelles

O-O-18 Formations proposées aux administrateurs par les formateurs du fournisseur

O-O-19 Formations proposées aux administrateurs par des prestataires externes, par exemple des associations industrielles, TÜV (Agence de contrôle technique)

O-O-20 Matériel d'auto-apprentissage pour les administrateurs, par exemple des vidéos tutoriels, des présentations, des instructions étape par étape

O-O-21 Manuels d'utilisation pour l'administrateur

O-O-22 Manuels d'administration basés sur des scénarios

8.8 Architecture logicielle

Risque visé : Si l'accès à l'infrastructure de BASF est autorisé depuis l'extérieur via Internet, les attaquants pourraient exploiter les vulnérabilités fonctionnelles et architecturales pour récupérer des données ou, en cas d'attaque réussie, accéder à d'autres systèmes au sein de l'infrastructure BASF via une augmentation des privilèges.

Objectif : L 'architecture et les processus de traitement des données sont conçus pour protéger la solution et les données traitées contre tout accès non autorisé, et pour garantir qu'aucun autre système BASF n'est affecté si des composants individuels sont compromis.

Mesures techniques

O-T-19 Architecture à 3 niveaux : séparation des couches de présentation, de traitement et de stockage des données

O-T-20 Architecture à 2 niveaux : séparation des couches applicatives et de stockage des données

O-T-21	Protection contre le cross-site scripting
O-T-22	Validation des entrées pour se protéger contre toute manipulation non autorisée des données, par exemple via une injection SQL

Mesures organisationnelles

O-O-23	Documentation de l'architecture de la solution

9 Solutions cloud

Explication : Achat d'applications (packages) qui sont exploitées dans l'infrastructure d'un fournisseur de services et dont l'utilisation nécessite un accès obligatoire à Internet. Peu importe qu'il s'agisse d'une solution SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service), Iaas (Infrastructure-as-aService) ou d'une technologie cloud qui n'est pas spécifiée ici.

9.1 Concept de sécurité informatique

Risque visé : Si les mécanismes de sécurité standards dans l'industrie ne sont pas pris en compte lors de la planification et du développement, ou si les interactions entre les mesures ne sont pas identifiées, les attaquants pourraient exploiter les vulnérabilités qui en résultent et compromettre les informations, les données et l'infrastructure de BASF.

Objectif : L'ensemble des mesures de sécurité d'une solution est défini dans le cadre d'un concept de sécurité informatique. Le statut de l'implémentation est documenté et mis à jour en permanence lorsque des modifications sont apportées.

Mesures organisationnelles

Référence CL-O-01 Développement d'un concept de sécurité informatique pour la solution

---

Référence CL-O-02 Mise à jour régulière du concept de sécurité informatique, notamment en cas de modifications

---

Référence CL-O-03 Fourniture à BASF de la documentation sur les mécanismes de sécurité mis en œuvre

9.2 Cryptographie

Risque visé : Si les données ne sont pas protégées pendant le stockage, le traitement ou la transmission, elles pourraient être interceptées ou compromises par des tiers non autorisés.

Objectif : Tout au long du cycle de vie, les données sont protégées contre tout accès non autorisé.

Mesures techniques

Référence CL-T-01 Cryptage des données lors du transfert (Data at Transit), par exemple HTTPS, SSH

Référence CL-T-02 Cryptage des données pendant le stockage, par exemple cryptage de la base de données

Référence CL-T-03 Authentification multi facteurs pour l'accès aux informations sensibles

Référence CL-T-04 Authentification multi facteurs pour les modifications de configuration

Mesures organisationnelles

Référence CL-O-04 Concept de cryptographie avec toutes les méthodes de cryptage mises en œuvre et les longueurs de clé

9.3 Concept en matière de rôles et d'autorisation

Risque visé : Un concept de rôles et d'autorisations manquant ou incorrect pourrait permettre à des utilisateurs non autorisés d'accéder à des informations sensibles.

Objectif : Les rôles et les autorisations peuvent être gérés de manière granulaire afin que les utilisateurs n'aient accès qu'aux informations dont ils ont besoin pour effectuer leurs tâches.

Mesures techniques

Référence CL-T-05 Active Directory API

Référence CL-T-06 LDAP API

Référence CL-T-07 Attribution d'autorisations exclusivement via l'attribution de rôles

Référence CL-T-08 Module logiciel / composant / fonction pour la gestion des rôles et des autorisations

Mesures organisationnelles

Référence CL-O-05 Concept formalisé et documenté de rôles et d'autorisations

9.4 Protection contre les logiciels malveillants

Risque visé : Si les systèmes sont compromis, des informations pourraient être modifiées par inadvertance ou rendues accessibles à des tiers non autorisés.

Objectif : Garantir qu'aucun logiciel malveillant ne puisse être installé sur les appareils informatiques.

Mesures techniques

Réf CL-T-09 Solution de protection contre les logiciels malveillants pour les serveurs Windows

---

Réf. CL-T-10 Solution de protection contre les logiciels malveillants sur les clients, par exemple Microsoft Defender

---

Réf. CL-T-11 Appareils de sécurité, par ex. Pare-feu, SIEM

CL-T-12 Segmentation appropriée du réseau de l'entreprise en fonction de la criticité en matière de confidentialité et de disponibilité des données traitées

---

CL-T-13 Utilisation d'une solution de bac à sable pour ouvrir des fichiers inconnus ou des fichiers provenant d'expéditeurs inconnus.

CL-T-14 Distribution des logiciels gérée de manière centralisée

---

CL-T-15 Interdiction d'accorder des droits d'administration locale aux développeurs

---

CL-T-16 Pas d'octroi de droits d'administration locale aux utilisateurs

Mesures organisationnelles

CL-O-06 Processus pour l'installation immédiate des mises à jour des logiciels quand elles concernent la sécurité

Réf CL-O-07 Politique de renforcement des serveurs

Réf CL-O-08 Politique de renforcement des clients
CL-O-09 Politique de renforcement des smartphones

9.5 Sauvegarde des données

Risque visé : Les erreurs système, les logiciels malveillants ou l'utilisation abusive des systèmes informatiques peuvent entraîner la perte de données.

Objectif : Toutes les données pertinentes pour BASF sont sauvegardées régulièrement et peuvent être restaurées en cas de perte.

Mesures techniques

CL-T-17 Sauvegarde régulière et automatisée de toutes les données pertinentes pour BASF

CL-T-18 Workflow de déploiement automatisé, par exemple CI/CD

Mesures organisationnelles

CL-O-10 Concept de sauvegarde des données

CL-O-11 Exercices réguliers de sauvegarde et de récupération de données

CL-O-12 Faire des instantanés manuels de l'état du système avant d'apporter des modifications importantes aux systèmes et aux applications qui sont nécessaires à l'exécution de la solution

9.6 Tests d'intrusion

Risque visé : La complexité des solutions peut faire que les vulnérabilités passent inaperçues en raison de l'interaction des sous-composants et des effets qui en résultent. Ces angles morts pourraient être exploités par les attaquants.

Objectif : Le niveau de protection de l'ensemble de la solution est régulièrement réexaminé en tenant compte de toutes les méthodes d'attaque connues. En fonction des résultats, le niveau de protection sera redéveloppé.

Mesures organisationnelles

CL-O-13 Des tests d'intrusion réguliers de la solution

CL-O-14 Tests d'intrusion de la solution mis en place lors d'événements, par exemple en cas de modifications importantes

---

CL-O-15 Tests d'intrusion réguliers de composants tiers, par exemple des modules logiciels de développeurs externes

---

CL-O-16 Tests d'intrusion de composants tiers mis en place lors d'événements, par exemple, lorsque des vulnérabilités ou des incidents de sécurité sont identifiés

9.7 Support et documentation pour les utilisateurs

Risque visé : Des instructions utilisateur manquantes ou indisponibles peuvent entraîner une non-utilisation ou une utilisation incorrecte de la solution. Cela pourrait avoir un effet négatif sur les activités de BASF.

Objectif : Tous les groupes d'utilisateurs ont la possibilité d'utiliser la solution de la manière prévue pour l'usage prévu.

Mesures techniques

CL-T-19 Forum communautaire d'échange entre utilisateurs

CL-T-20 Site web d'assistance pour les utilisateurs

CL-T-21 Hotline téléphonique pour les utilisateurs

CL-T-22 Assistance par e-mail pour les utilisateurs

Mesures organisationnelles

CL-O-17 Formations proposées aux utilisateurs par les formateurs du fournisseur

CL-O-18 Formations proposées aux utilisateurs par des prestataires externes, par exemple des associations industrielles, TÜV (Association allemande de contrôle technique)

CL-O-19 Matériel d'auto-apprentissage pour l'utilisateur, par exemple des vidéos tutoriels, présentations, instructions étape par étape

CL-O-20 Manuels d'utilisation

CL-O-21 Manuels d'utilisation basés sur des scénarios

9.8 Support et documentation pour les administrateurs

Risque visé : L'installation, la distribution ou une configuration incorrecte peuvent entraîner la compromission des données ou la défaillance de la solution, perturbant ainsi les activités de BASF.

Objectif : Les administrateurs BASF responsables de l'exploitation de la solution ont la possibilité de gérer la solution comme prévu.

Mesures techniques

CL-T-23	Forum communautaire d'échange entre administrateurs
CL-T-24	Site web d'assistance pour les administrateurs
CL-T-25	Hotline téléphonique pour les administrateurs
CL-T-26	Assistance par e-mail pour les administrateurs

Mesures organisationnelles

CL-O-22	Formations proposées aux administrateurs par les formateurs du fournisseur
CL-O-23	Formations proposées aux administrateurs par des prestataires externes, par exemple des associations industrielles, TÜV (Agence de contrôle technique)
CL-O-24	Matériel d'auto-apprentissage pour les administrateurs, p. ex. des vidéos tutoriels, présentations, instructions étape par étape
CL-O-25	Manuels d'utilisation pour de l'administrateur
CL-O-26	Manuels d'administration basés sur des scénarios

9.9 Architecture logicielle

Risque visé : Les attaquants pourraient exploiter les vulnérabilités de l'architecture logicielle pour récupérer des données ou, en cas d'attaque réussie, accéder à d'autres systèmes de l'infrastructure BASF par le biais d'une augmentation de privilèges.

Objectif : L'architecture logicielle est conçue pour protéger la solution et les données traitées contre tout accès non autorisé, et pour s'assurer qu'aucun autre système BASF n'est affecté si des composants individuels sont compromis.

Mesures techniques

CL-T-27	Architecture à 3 niveaux : séparation des couches de présentation, de traitement et de stockage des données
CL-T-28	Architecture à 2 niveaux : séparation des couches applicatives et de stockage des données
CL-T-29	Protection contre le cross-site scripting
CL-T-30	Validation des entrées pour se protéger contre toute manipulation non autorisée des données, par exemple via une injection SQL

Mesures organisationnelles

CL-O-27	Documentation de l'architecture de la solution

9.10 Gestion de la continuité des activités

Risque visé : La défaillance ou le dysfonctionnement de composants critiques du système peuvent entraîner l'indisponibilité des solutions cloud. En particulier dans le cas de processus commerciaux critiques, même une panne de courte durée peut entraîner des dommages considérables pour BASF.

Objectif : Le respect des accords de niveau de service (SLA) peut être garanti pendant toute la durée du contrat.

Mesures techniques	
CL-T-31	Centre de données secondaire
Mesures organisationnelles	
CL-O-28	Nomination d'une personne responsable de la gestion de crise, p. ex. agent de GCA, agent d'urgence
CL-O-29	Gestion de l'ensemble des mesures de gestion des urgences dans le cadre d'un système de management de la continuité des activités (SMCA)
CL-O-30	Concept de redondance

9.11 Protection des informations personnelles (PII)

Risque visé : Lors du traitement d'informations personnelles dans le cadre du contrat, les droits de certaines personnes peuvent être compromis par une utilisation inappropriée des informations.

Objectif : Lors du traitement des données personnelles, il est garanti à tout moment que les exigences du RGPD et des réglementations en aval sur la protection des données sont respectées.

Mesures organisationnelles

CL-O-31	Nomination d'une personne responsable de la protection des données, par exemple un délégué à la protection des données
CL-O-32	Protection de l'ensemble des renseignements personnels identifiables dans le cadre d'un système de gestion de la protection des données (SGD)

9.12 Sécurité physique

Risque visé : Si les solutions cloud sont exploitées dans des centres de données non sécurisés, les serveurs et autres composants informatiques peuvent être manipulés, volés ou détruits.

Objectif : Toute l'infrastructure requise pour fournir la solution cloud est exploitée dans un centre de données sécurisé.

Mesures techniques

CL-T-32	Système d'extinction et de prévention des incendies
CL-T-33	Plusieurs compartiments coupe-feu
CL-T-34	Système d'alarme de danger
CL-T-35	Système de vidéosurveillance

CL-T-36 Surveillance automatisée de l'infrastructure

CL-T-37 Connexion du centre de données à un poste de contrôle central, 24h/24 et 7j/7

CL-T-38 Gestion de la température et de l'humidité

CL-T-39 Alimentation électrique sans coupure

CL-T-40 Dispositif de protection contre les surtensions

Mesures organisationnelles

CL-O-33 Mesures de protection contre la poussière

CL-O-34 Concept de contrôle d'accès

10 Développement de logiciels

Description : Développement de solutions logicielles ou de composants utilisés de manière autonome ou en intégration avec d'autres solutions. Cela inclut également la personnalisation des solutions. La configuration d'une solution ne relève pas du développement de logiciel.

Remarque sur l'application : Quand le fournisseur développe la solution lui-même, il doit remplir les exigences de ce chapitre et, en plus, celles des chapitres Solutions locales et Solutions cloud.

10.1 Processus de développement

Risque visé : Si les règles de l'art en matière de développement de logiciels sécurisés ne sont pas appliquées, des vulnérabilités de sécurité peuvent être générées que des attaquants pourraient exploiter. Cela s'applique à la fois au code source et à la configuration du support d'installation fourni.

Objectif : Un processus de développement standardisé et géré garantit que toutes les vulnérabilités connues dans les logiciels (packages) utilisés sont bloquées et que les supports d'installation sont configurés de manière suffisamment sécurisée avant le déploiement.

Mesures techniques

SW-T-01 Workflow de déploiement automatisé, par exemple CI/CD

Mesures organisationnelles	
SW-O-01	Cycle de vie formalisé du développement logiciel sécurisé (SSDLC)
SW-O-02	Gestion et documentation des outils utilisés dans le processus de développement
SW-O-03	Tester les nouvelles versions de la solution sur la base de « test case » standardisés
SW-O-04	Réalisation de tests unitaires
SW-O-05	Réalisation d'essais de montée en charge
SW-O-06	Respect du principe : Sécurité dès la conception
SW-O-07	Respect du principe : Sécurité par défaut

SW-O-08 Respect du principe : Privacy by Design
SW-O-09 Respect du principe de la protection de la vie privée par défaut

10.2 Logiciels tiers

Risque visé : Lors de l'utilisation de composants logiciels tiers, tels que des modules logiciels de développeurs externes, les vulnérabilités de ces composants peuvent servir de vecteurs d'attaque aux attaquants pour leur permettre d'obtenir un accès non autorisé aux données.

Objectif : Tous les composants logiciels tiers sont régulièrement vérifiés pour détecter les vulnérabilités. Les mises à jour et les correctifs de sécurité des composants externes sont fournis par le fournisseur via le canal général des mises à jour et des correctifs convenu pour la solution.

Mesures organisationnelles
SW-O-10 Registre de tous les composants logiciels de tiers
SW-O-11 Processus de test périodique pour détecter les vulnérabilités connues des composants logiciels tiers utilisés.