BASF-Gruppe –
Addendum zur Cybersicherheit

Version	**5.1**
Klassifizierung	**P U B L I C**

Versionsdetails

Version	5.1
Erstellt durch	Sebastian Krüsmann, NeoMINT GmbH
Status	Freigegeben
Freigegeben am	10.01.2024
Freigegeben durch	Julia Mansky, BASF Digital Solutions GmbH
Updates unter	Download Center (basf.com)

Historie

Version	Datum	Erstellt durch	Änderungen
5.0	08.01.2024	Sebastian Krüsmann, NeoMINT GmbH	Initiale Erstellung
5.1	08.08.2024	Beatrice Huck, NeoMint GmbH	Maßnahmen C-T-12, S-T-12 und CL-T-15 hinzugefügt Maßnahmen C-T-13, S-T-13, CL-T-16, CL-T-09, C-T-06 und S-T-06 geändert

Inhaltsverzeichnis

1 Haftungsausschluss

Das Security Addendum enthält Anforderungen an die Informationssicherheit.

Alle IT-Lieferanten müssen die Vorgaben im Kapitel "Allgemeines" erfüllen. Die **weiteren Anforderungen** sind **nach Lieferantentypen getrennt** und sollten entsprechend erfüllt werden. Eine Erläuterung der Lieferantentypen finden Sie am Anfang des jeweiligen Kapitels.

Für jeden Lieferantentyp gibt es Kapitel, in denen die spezifischen Risiken und das Ziel, das mit der Bewältigung des Risikos erreicht werden soll, beschrieben werden. Dazu gibt es verschiedene Maßnahmen technischer oder organisatorischer Art, die in der Regel angewendet werden können. Für den Fall, dass das Risiko im konkreten Fall nicht relevant ist oder ein Lieferant der Meinung ist, dass ein Risiko anders als angegeben behandelt werden kann, besteht die Möglichkeit, dies kurz zu erläutern. Es obliegt der BASF zu entscheiden, ob die angegebenen Gründe und Maßnahmen ausreichend sind.

2 Ansprechpartner für Cyber Security

Um eine reibungslose und effiziente Zusammenarbeit mit unseren IT-Lieferanten zur Aufrechterhaltung eines angemessenen Cyber Security-Niveaus sicherzustellen, sind von jedem Lieferanten Ansprechpartner und Kontaktinformationen für Kernrollen der Cyber Security zu benennen.

Die Informationen werden durch den internen Auftraggeber (iBP oder Einkauf) im Formular *2 IT-Supplier Security Assessment_EN_Contact Sheet* in der jeweils aktuellen Version in deutscher oder englischer Sprache für jeden Lieferanten dokumentiert und an das Supplier Security-Team übermittelt.

3 Allgemein

Die allgemeine Sicherheit des Lieferanten ist relevant, wenn die Risiken unabhängig von der erbrachten Dienstleistung bestehen.

3.1 (Einheitlicher) Ansprechpartner (SPoC) für Cybersicherheit / Informationssicherheit

Angesprochenes Risiko Eine unzureichende oder verzögerte Kommunikation mit den Lieferanten über Fragen der Cybersicherheit könnte dazu führen, dass Schwachstellen zu spät oder unzureichend angegangen werden.

Ziel Anfragen zu Fragen der Cybersicherheit, z.B. zu implementierten Sicherheitsmaßnahmen oder bei Bekanntwerden von Sicherheitsvorfällen, die den Lieferanten betreffen, werden innerhalb einer angemessenen Zeitspanne beantwortet.

Technische Maßnahmen	
G-T-01	Plattform, über die Anfragen eingereicht und zeitnah beantwortet werden, z.B. Ticketsystem

Organisatorische Maßnahmen	
G-O-01	Ansprechpartner für Fragen der Cybersicherheit, z. B. CISO / Informationssicherheitsbeauftragter

3.2 Personelle Sicherheit

Adressiertes Risiko Die Mitarbeiter von Lieferanten könnten durch ihr Verhalten, sowohl absichtlich als auch durch Unachtsamkeit, einen erheblichen negativen Einfluss auf das Sicherheitsniveau der BASF haben.

Ziel Nur ausreichend qualifizierte und informierte Mitarbeiter erhalten Zugang zu Informationen oder Systemen der BASF.

Technische Maßnahmen	
G-T-02	Rollen- und Berechtigungskonzept: Mitarbeiter erhalten nur Zugang zu Informationen, die für ihre Arbeit relevant sind (Need-to-know-Prinzip)

Organisatorische Maßnahme	
G-O-02	Regelmäßige Sensibilisierungsschulungen zu Cybersicherheitsthemen für alle Mitarbeiter

3.3 Management der Informationssicherheit

Adressiertes Risiko Eine unzureichende Konzeption und Operationalisierung der Cybersicherheit könnte dazu führen, dass Schwachstellen nicht frühzeitig erkannt oder vermieden werden. Die Ausnutzung solcher Schwachstellen durch einen Angreifer könnte sich negativ auf das Sicherheitsniveau der BASF auswirken.

Ziel Proaktive Gestaltung und Verwaltung der Gesamtheit der Sicherheitsmechanismen des Lieferanten.

Organisatorische Maßnahmen	
G-O-03	Benennung einer Person, die für die Aufrechterhaltung eines angemessenen Niveaus der Cybersicherheit verantwortlich ist, z. B. CISO oder Informationssicherheitsbeauftragter
G-O-04	Management der Gesamtheit aller Cybersicherheitsmaßnahmen im Rahmen eines Informationssicherheitsmanagementsystems (ISMS)
G-O-05	Zertifizierung des Informationssicherheits-Managementsystems auf der Grundlage einer etablierten Norm, z. B. ISO 27001

3.4 Sicherheit der Lieferkette

Adressiertes Risiko Eine unzureichende Konzeption und Operationalisierung der Cybersicherheit könnte dazu führen, dass Schwachstellen nicht frühzeitig erkannt oder vermieden werden. Die Ausnutzung solcher Schwachstellen durch einen Angreifer könnte sich negativ auf das Sicherheitsniveau der BASF auswirken.

Ziel Alle wesentlichen Unterauftragnehmer und Zulieferer sollen verpflichtet werden, ein angemessenes Niveau der Cybersicherheit zu schaffen und aufrechtzuerhalten.

Organisatorische Maßnahmen	
G-O-06	Register der Unterlieferanten, die für die Erbringung von Dienstleistungen für BASF tätig sind
G-O-07	Vertragliche Verpflichtung von Unterauftragnehmern und Lieferanten, ein angemessenes Niveau der Cybersicherheit zu schaffen und aufrechtzuerhalten

3.5 Änderungsmanagement

Adressiertes Risiko Eine unzureichende Kontrolle von Änderungen an den bereitgestellten Dienstleistungen und Produkten könnte zu Informationsverlusten und Leistungseinbußen führen, was sich negativ auf die Geschäftstätigkeit der BASF auswirken könnte.

Ziel Einführung eines standardisierten und formalisierten Verfahrens für die Koordinierung von Änderungen an den angebotenen Dienstleistungen und Produkten sowie für deren Umsetzung.

Technische Maßnahmen	
G-T-03	Plattform, über die alle Vertrags- und Serviceänderungen verwaltet und dokumentiert werden

Organisatorische Maßnahmen	
G-O-08	(Einheitlicher) Ansprechpartner (SPoC) für Änderungen an den vertraglich vereinbarten Dienstleistungen

3.6 Einhaltung der Vorschriften

Adressiertes Risiko BASF könnte für von Lieferanten verursachten Verstöße gegen Gesetze und Vorschriften haftbar gemacht werden.

Ziel Alle geltenden Compliance-Anforderungen werden jederzeit eingehalten.

Organisatorische Maßnahmen	
G-O-09	Benennung einer Person, die für die Aufrechterhaltung der globalen Compliance verantwortlich ist, z. B. eines Compliance-Beauftragten
G-O-10	Verwaltung aller Compliance-Maßnahmen im Rahmen eines Compliance-Management-Systems (CMS)

4 Beratungsdienste

Alle Beratungsleistungen, die direkt oder indirekt mit der Organisationsentwicklung sowie der Bereitstellung, dem Betrieb oder der Stilllegung von IT-Lösungen zusammenhängen.

4.1 Ressourcenmanagement

Adressiertes Risiko Personalmangel könnte dazu führen, dass vertraglich vereinbarte Leistungen nicht erbracht werden.

Ziel Es ist jederzeit gewährleistet, dass ausreichend qualifizierte Mitarbeiter für die Erbringung der vertraglich vereinbarten Leistungen zur Verfügung stehen. Alle Leistungen können pünktlich und in der vereinbarten Qualität erbracht werden.

Organisatorische Maßnahmen	
C-O-01	Verwaltung der personellen Ressourcen im Rahmen des internen Ressourcenmanagements zur Bereitstellung von qualifiziertem Personal
C-O-02	Aus- und Weiterbildungskonzept für Fach- und Führungskräfte

4.2 Umgang mit Informationen

Adressiertes Risiko Informationen, die im Rahmen von Beratungsprojekten verwendet werden, könnten die Cybersicherheit von BASF gefährden, wenn die Vertraulichkeit verloren geht.

Ziel Es ist jederzeit sichergestellt, dass alle Informationen, die im Rahmen von Beratungsprojekten entstehen und eingehen, vertraulich behandelt und vor Kompromittierung geschützt werden.

Technische Maßnahmen	
C-T-01	Verschlüsselung der E-Mail-Kommunikation mit einem etablierten Industriestandard, z. B. PGP, S/MIME
C-T-02	Verschlüsselung von Festplatten mobiler Geräte, z. B. BitLocker, Vera Crypt
C-T-03	Verschlüsselung von Server-Festplatten, z. B. BitLocker, Vera Crypt

C-T-04	Verschlüsselung von mobilen Datenträgern, z.B. BitLocker, Vera Crypt, Hardware-Verschlüsselung
C-T-05	Verwaltung aller Berechtigungen im Rahmen eines durchgängigen Identitäts- und Zugriffsmanagements (IAM)

Organisatorische Maßnahmen

C-O-03	Richtlinie zur Speicherung, Verarbeitung und Übermittlung von Informationen vor, während und nach Projekten
C-O-04	Prozess zur Behandlung von Sicherheitsvorfällen
C-O-05	Prozess zur Fernlöschung von Daten bei Verlust von mobilen Geräten
C-O-06	Prozess, der sicherstellt, dass nur Mitarbeiter, die Beratungsleistungen für BASF erbringen, Zugang zu BASF-Informationen haben (Need-to-know-Prinzip)
C-O-07	Verfahren für die Gewährung, Änderung oder den Entzug von Zugriffsrechten, wenn Mitarbeiter in das Unternehmen eintreten, es verlassen oder die Rolle wechseln (Joiner-Mover-Leaver-Prozess)
C-O-08	Klassifizierungskonzept für verarbeitete Informationen auf der Grundlage ihrer Kritikalität

4.3 Schutz vor Malware

Adressiertes Risiko Wenn die im Beratungsprozess verwendeten IT-Geräte kompromittiert werden, könnten Informationen unbeabsichtigt verändert oder unbefugten Dritten zugänglich gemacht werden.

Ziel Es wird sichergestellt, dass keine Schadsoftware auf den IT-Geräten installiert werden kann.

Technische Maßnahmen	
C-T-06	Lösung zum Schutz vor Malware für Windows Server
C-T-07	Lösung zum Schutz vor Malware auf den Clients, z. B. Microsoft Defender
C-T-08	Sicherheitsvorrichtungen, z. B. Firewall, SIEM
C-T-09	Geeignete Segmentierung des Unternehmensnetzes auf der Grundlage der Kritikalität der Anforderungen an die Vertraulichkeit und Verfügbarkeit der verarbeiteten Daten
C-T-10	Verwendung einer Sandbox-Lösung zum Öffnen unbekannter Dateien oder Dateien von unbekannten Absendern.
C-T-11	Zentral verwaltete Softwareverteilung
C-T-12	Keine Vergabe von lokalen Administratorrechten an Benutzer
C-T-13	Keine Vergabe von lokalen Administratorrechten an Entwickler
Organisatorische Maßnahmen	
C-O-09	Prozess zur sofortigen Installation von sicherheitsrelevanten Updates aller eingesetzten Softwarelösungen
C-O-10	Härtungsrichtlinie für Server
C-O-11	Härtungsrichtlinie für Clients
C-O-12	Härtungsrichtlinie für Smartphones

4.4 Datensicherung

Angesprochenes Risiko Systemfehler, Schadsoftware oder Missbrauch von IT-Systemen könnten zum Verlust von Daten führen, die im Rahmen eines Beratungsprojekts erhoben wurden.

Ziel Alle für die BASF relevanten Daten werden regelmäßig gesichert und können im Falle eines Datenverlustes wiederhergestellt werden.

Technische Maßnahmen	
C-T-14	Regelmäßige, automatisierte Sicherung aller für die BASF relevanten Daten

Organisatorische Maßnahmen	
C-O-13	Datensicherungskonzept
C-O-14	Regelmäßige Übungen zur Datensicherung und -wiederherstellung

4.5 Physische Sicherheit

Angesprochenes Risiko Bei der Verarbeitung in den Räumlichkeiten des Lieferanten könnten BASF-Informationen durch externe Parteien kompromittiert werden.

Ziel Alle Informationen von und über BASF sind vor dem physischen Zugriff unbefugter Dritter geschützt.

Technische Maßnahmen	
C-T-15	Verschließbare Büros
C-T-16	Verschließbare Schränke oder Tresore

Organisatorische Maßnahmen	
C-O-15	Richtlinie in Bezug auf die Begleitung von Gästen in den Liegenschaften des Lieferanten durch Mitarbeiter
C-O-16	Richtlinie zum Verschluss von Datenträgern, IT-Geräten und Dokumenten

4.6 Schutz von personenbezogenen Daten (PII)

Angesprochenes Risiko Bei der Verarbeitung personenbezogener Daten im Rahmen der Auftragsverarbeitung könnten die Persönlichkeitsrechte der betroffenen Personen durch eine unsachgemäße Verwendung der Informationen beeinträchtigt werden.

Ziel Bei der Verarbeitung von PII wird jederzeit sichergestellt, dass die Anforderungen der DSGVO und nachgelagerter Datenschutzbestimmungen eingehalten werden.

Organisatorische Maßnahmen	
C-O-17	Benennung einer für den Datenschutz verantwortlichen Person, z. B. eines Datenschutzbeauftragten
C-O-18	Schutz der Gesamtheit aller personenbezogenen Daten im Rahmen eines Datenschutzmanagementsystems (DMS)

5 Service und Unterstützung

Alle Service- und Supportleistungen, in deren Rahmen Lösungen verwaltet, gewartet oder ausgegliedert werden. Dies umfasst den gesamten Produktlebenszyklus einer Lösung und beginnt mit der Installation und endet mit der Ausgliederung.

5.1 Ressourcenmanagement

Angesprochenes Risiko Personalmangel könnte dazu führen, dass vertraglich vereinbarte Leistungen nicht erbracht werden.

Ziel Es ist jederzeit gewährleistet, dass ausreichend qualifizierte Mitarbeiter für die Erbringung der vertraglich vereinbarten Leistungen zur Verfügung stehen. Alle Leistungen können pünktlich und in der vereinbarten Qualität erbracht werden.

Organisatorische Maßnahmen	
S-O-01	Verwaltung der personellen Ressourcen im Rahmen des internen Ressourcenmanagements zur Bereitstellung von qualifiziertem Personal
S-O-02	Aus- und Weiterbildungskonzept für Fach- und Führungskräfte

5.2 Umgang mit Informationen

Adressiertes Risiko Informationen, die im Rahmen von Dienstleistungs- und Unterstützungsaufträgen verwendet werden, könnten die Cybersicherheit von BASF gefährden, wenn die Vertraulichkeit verloren geht.

Ziel Es ist jederzeit sichergestellt, dass alle Informationen, die im Rahmen von Dienstleistungen und Unterstützungstätigkeiten entstehen und eingehen, vertraulich behandelt und vor Kompromittierung geschützt werden.

Technische Maßnahmen	
S-T-01	Verschlüsselung der E-Mail-Kommunikation mit einem etablierten Industriestandard, z. B. PGP, S/MIME
S-T-02	Verschlüsselung von Festplatten mobiler Geräte, z. B. BitLocker, Vera Crypt
S-T-03	Verschlüsselung von Serverfestplatten, z. B. BitLocker, Vera Crypt

S-T-04	Verschlüsselung von mobilen Datenträgern, z.B. BitLocker, Vera Crypt, Hardware-Verschlüsselung
S-T-05	Verwaltung aller Berechtigungen im Rahmen eines durchgängigen Identitäts- und Zugriffsmanagements (IAM)

Organisatorische Maßnahmen

S-O-03	Richtlinie für die Speicherung, Verarbeitung und Übermittlung von Informationen vor, während und nach Projekten
S-O-04	Prozess zur Behandlung von Sicherheitsvorfällen
S-O-05	Prozess zur Fernlöschung von Daten bei Verlust von mobilen Geräten
S-O-06	Prozess, der sicherstellt, dass nur Mitarbeiter, die Beratungsleistungen für BASF erbringen, Zugang zu BASF-Informationen haben (Need-to-know-Prinzip)
S-O-07	Prozess für die Gewährung, Änderung oder den Entzug von Zugriffsrechten, wenn Mitarbeiter in das Unternehmen eintreten, es verlassen oder die Rolle wechseln (Joiner-Mover-Leaver-Prozess)
S-O-08	Klassifizierungskonzept für verarbeitete Informationen auf der Grundlage ihrer Kritikalität

5.3 Schutz vor Malware

Adressiertes Risiko Wenn IT-Geräte, die im Rahmen von Service- und Support-Aufgaben eingesetzt werden, kompromittiert werden, könnten Informationen unbeabsichtigt verändert oder unbefugten Dritten zugänglich gemacht werden.

Ziel Es wird sichergestellt, dass keine Schadsoftware auf den IT-Geräten installiert werden kann.

Technische Maßnahmen	
S-T-06	Lösung zum Schutz vor Malware für Windows Server
S-T-07	Lösung zum Schutz vor Malware auf den Clients, z. B. Microsoft Defender
S-T-08	Sicherheitsvorrichtungen, z. B. Firewall, SIEM
S-T-09	Geeignete Segmentierung des Unternehmensnetzes auf der Grundlage der Kritikalität der Anforderungen an die Vertraulichkeit und Verfügbarkeit der verarbeiteten Daten
S-T-10	Verwendung einer Sandbox-Lösung zum Öffnen unbekannter Dateien oder Dateien von unbekannten Absendern.
S-T-11	Zentral verwaltete Softwareverteilung
S-T-12	Keine Vergabe von lokalen Administratorrechten an Benutzer
S-T-13	Keine Vergabe von lokalen Administratorrechten an Entwickler
Organisatorische Maßnahmen	
S-O-09	Prozess zur sofortigen Installation von sicherheitsrelevanten Updates aller eingesetzten Softwarelösungen
S-O-10	Härtungsrichtlinie für Server
S-O-11	Härtungsrichtlinie für Clients
S-O-12	Härtungsrichtlinie für Smartphones

5.4 Datensicherung

Adressiertes Risiko Systemfehler, Schadsoftware oder Missbrauch von IT-Systemen könnten zum Verlust von BASF-relevanten Daten führen.

Ziel Alle für die BASF relevanten Daten werden regelmäßig gesichert und können im Falle eines Datenverlustes wiederhergestellt werden.

Technische Maßnahmen	
S-T-14	Regelmäßige, automatisierte Sicherung aller für die BASF relevanten Daten

Organisatorische Maßnahmen	
S-O-13	Datensicherungskonzept
S-O-14	Regelmäßige Übungen zur Datensicherung und -wiederherstellung

5.5 Physische Sicherheit

Adressiertes Risiko Bei der Verarbeitung in den Räumlichkeiten des Lieferanten könnten BASF-Informationen durch externe Parteien kompromittiert werden.

Ziel Alle Informationen von und über BASF sind vor dem physischen Zugriff unbefugter Dritter geschützt.

Technische Maßnahmen	
S-T-15	Verschließbare Büros
S-T-16	Verschließbare Schränke oder Tresore

Organisatorische Maßnahmen	
S-O-15	Richtlinie in Bezug auf die Begleitung von Gästen in den Liegenschaften des Lieferanten durch Mitarbeiter
S-O-16	Richtlinie zum Verschluss von Datenträgern, IT-Geräten und Dokumenten

5.6 Schutz von personenbezogenen Daten (PII)

Adressiertes Risiko Bei der Verarbeitung personenbezogener Daten im Rahmen der Auftragsverarbeitung könnten die Persönlichkeitsrechte der betroffenen Personen durch eine unsachgemäße Verwendung der Informationen beeinträchtigt werden.

Ziel Bei der Verarbeitung von PII wird jederzeit sichergestellt, dass die Anforderungen der DSGVO und nachgelagerter Datenschutzbestimmungen eingehalten werden.

Organisatorische Maßnahmen	
S-O-17	Benennung einer für den Datenschutz verantwortlichen Person, z. B. eines Datenschutzbeauftragten
S-O-18	Schutz der Gesamtheit aller personenbezogenen Daten im Rahmen eines Datenschutzmanagementsystems (DMS)

5.7 Fernzugriff

Adressiertes Risiko Fernzugriffssitzungen könnten von Unbefugten als Einfallstor in das BASF-Netzwerk genutzt werden. Unsichere Protokolle, Konfigurationen, Passwörter und Anwendungen könnten unbefugten Zugriff ermöglichen.

Ziel Bei jedem Fernzugriff ist der Schutz der gespeicherten, verarbeiteten und übertragenen Informationen und Daten sowie die Integrität der BASF-Infrastruktur gewährleistet.

Technische Maßnahmen	
S-T-17	Verwendung von sicheren Protokollen, Verschlüsselungsmethoden und Anwendungen beim Zugriff auf Daten und Infrastruktur der BASF

Organisatorische Maßnahmen	
S-O-19	Vollständige Dokumentation oder Aufzeichnung aller Fernzugriffssitzungen

5.8 IT-Administration

Adressiertes Risiko Eine unsachgemäße IT-Administration könnte zu einer Störung oder Beeinträchtigung der BASF-Infrastruktur führen.

Ziel Alle Service- und Support-Aktivitäten werden in Übereinstimmung mit den besten Praktiken der Branche für eine sichere Administration durchgeführt.

Technische Maßnahmen	
S-T-18	Ticketsystem für die Verwaltung von Service- und Supportanfragen

Organisatorische Maßnahmen	
S-O-20	Verwaltung und Dokumentation der vom Service- und Supportpersonal verwendeten Tools
S-O-21	Unverzügliche Installation von sicherheitsrelevanten Updates und Patches aller eingesetzten Softwarelösungen
S-O-22	Prozess zur Durchführung der erbrachten Service- und Supportleistungen.

6 Hardware-Komponenten

Beschaffung einzelner Hardwarekomponenten, die in Endgeräten installiert sind oder für deren Nutzung ein Endgerät benötigt wird, z.B. Maus, Tastatur, Bildschirm, RAM, Festplatten etc.

6.1 Lieferung

Adressiertes Risiko Hardwarekomponenten könnten während des Lieferprozesses beschädigt werden. Darüber hinaus könnten Komponenten manipuliert werden, um die BASF-Infrastruktur zu kompromittieren.

Ziel Alle Hardwarekomponenten werden voll funktionsfähig und in der vorgesehenen Konfiguration in einem einwandfreien Zustand geliefert.

Technische Maßnahmen	
H-T-01	Plattform für die Entgegennahme, Bearbeitung und Lösung von Beschwerden und Rücksendungen
H-O-01	Prozess zur Sicherstellung der Vollständigkeit jeder Lieferung vor dem Versand
Organisatorische Maßnahmen	
H-O-02	Sendungsverfolgung in Echtzeit
H-O-03	Schutz der Sendungen vor Beschädigung
H-O-04	Versiegelung aller Sendungen

6.2 Produktsicherheit

Adressiertes Risiko Ungeeignete, beschädigte oder manipulierte Komponenten könnten zu Störungen oder Beeinträchtigungen der BASF-Infrastruktur führen.

Ziel Alle Hardwarekomponenten werden vom Lieferanten oder einem Vorlieferanten auf ihre Funktionalität und Integrität geprüft. Für alle Hardwarekomponenten ist eine ausreichende technische Dokumentation vorhanden, um die optimalen Komponenten für eine bestimmte Anwendung auszuwählen.

Organisatorische Maßnahmen	
H-O-05	Dokumentation der idealen Betriebsumgebung für alle Komponenten
H-O-06	Prozess zur Validierung der Funktionalität und Integrität aller Komponenten durch den Lieferanten oder einen Vorlieferanten

7 Endpunkt & Geräte

Beschaffung von Geräten, die für den Einsatz bei Endnutzern oder im Rechenzentrum vorgesehen sind, z. B. Laptops, Smartphones, Server usw., sowie Appliances (Einzweckgeräte/Geräte mit spezialisierten Betriebssystemen, die für den Betrieb unerlässlich sind), wie Firewalls, VPN-Gateways, Router oder Switches.

7.1 Lieferung

Adressiertes Risiko Geräte könnten während des Lieferprozesses beschädigt werden. Darüber hinaus könnten Komponenten manipuliert werden, um die BASF-Infrastruktur zu kompromittieren.

Ziel Alle Produkte werden voll funktionsfähig und in der vorgesehenen Konfiguration in einem einwandfreien Zustand geliefert.

Technische Maßnahmen	
E-T-01	Plattform für die Entgegennahme, Bearbeitung und Lösung von Beschwerden und Rücksendungen
Organisatorische Maßnahmen	
E-O-01	Prozess zur Sicherstellung der Vollständigkeit jeder Lieferung vor dem Versand
E-O-02	Sendungsverfolgung in Echtzeit
E-O-03	Schutz der Sendungen vor Beschädigung
E-O-04	Versiegelung aller Sendungen

7.2 Produktsicherheit

Adressiertes Risiko Ungeeignete, beschädigte oder manipulierte Geräte könnten zu Störungen oder Kompromittierungen der BASF-Infrastruktur führen.

Ziel Alle Geräte werden vom Lieferanten oder einem Vorlieferanten auf ihre Funktionalität und Unversehrtheit geprüft. Für alle Hardwarekomponenten ist eine ausreichende technische Dokumentation vorhanden, um die optimalen Komponenten für eine bestimmte Anwendung auszuwählen.

Organisatorische Maßnahmen	
E-O-05	Dokumentation der idealen Betriebsumgebung für alle Komponenten
E-O-06	Prozess zur Validierung der Funktionalität und Integrität aller Komponenten durch den Lieferanten oder einen Vorlieferanten

7.3 Gerät einrichten

Adressiertes Risiko Bei der Ersteinrichtung von Geräten durch den Hersteller können Angreifer durch die Verwendung gängiger und daher leicht zu erratender Standardkonfigurationen BASF kompromittieren.

Ziel Sicherheitsbezogene Updates und Patches, die zum Zeitpunkt der Installation verfügbar sind, werden auf allen Geräten installiert. Initialpasswörter sind so konfiguriert, dass sie vom Benutzer bei der ersten Anmeldung geändert werden müssen.

Organisatorische Maßnahmen	
E-O-07	Installation aller verfügbaren Updates und Patches für das Betriebssystem und die Firmware
E-O-08	Verwendung von Initialpasswörtern, die bei der ersten Benutzung des Geräts geändert werden müssen
E-O-09	Vermeidung der Installation von Softwarepaketen, die nicht unbedingt erforderlich sind, z. B. optionale OEM-Software

8 On-Premise-Lösungen

Beschaffung von Anwendungen (Paketen), die auf der BASF-Infrastruktur (z.B. auf Laptops, Servern oder Smartphones) laufen und für deren Nutzung kein Zugriff auf die Systeme des Herstellers erforderlich ist.

8.1 IT-Sicherheitskonzept

Adressiertes Risiko Werden branchenübliche Sicherheitsmechanismen bei der Planung und Entwicklung nicht berücksichtigt oder werden die Wechselwirkungen zwischen den Maßnahmen nicht erkannt, könnten Angreifer die daraus resultierenden Sicherheitslücken ausnutzen und Informationen, Daten und Infrastruktur der BASF kompromittieren.

Ziel Im Rahmen eines IT-Sicherheitskonzepts wird die Gesamtheit aller Sicherheitsmaßnahmen für eine Lösung definiert und der Umsetzungsstand kontinuierlich dokumentiert und bei Änderungen aktualisiert.

Organisatorische Maßnahmen	
O-O-01	Entwicklung eines IT-Sicherheitskonzepts für die Lösung
O-O-02	Regelmäßige Aktualisierung des IT-Sicherheitskonzepts und bei Änderungen
O-O-03	Bereitstellung einer Dokumentation der implementierten Sicherheitsmechanismen für BASF

8.2 Kryptographie

Angesprochenes Risiko Wenn Daten während der Speicherung, Verarbeitung oder Übertragung nicht geschützt sind, könnten sie von unbefugten Dritten abgefangen oder kompromittiert werden.

Ziel Während des gesamten Lebenszyklus sind die Daten vor unbefugtem Zugriff geschützt.

Technische Maßnahmen	
O-T-01	Verschlüsselung von Daten während der Übertragung (Data at Transit), z. B. HTTPS, SSH
O-T-02	Verschlüsselung von Daten während der Speicherung, z. B. Datenbankverschlüsselung
O-T-03	Multi-Faktor-Authentifizierung für den Zugriff auf sensible Informationen
O-T-04	Multi-Faktor-Authentifizierung für Konfigurationsänderungen

Organisatorische Maßnahmen	
O-O-04	Krypto-Konzept mit allen implementierten Verschlüsselungsmethoden und Schlüssellängen

8.3 Rollen- und Berechtigungskonzept

Adressiertes Risiko Ein fehlendes oder unzureichendes Rollen- und Berechtigungskonzept könnte es unbefugten Benutzern ermöglichen, Zugang zu sensiblen Informationen zu erhalten.

Ziel Rollen und Berechtigungen können granular verwaltet werden, so dass die Benutzer nur auf die Informationen zugreifen können, die sie zur Erfüllung ihrer Aufgaben benötigen.

Technische Maßnahmen	
O-T-05	Active Directory-API
O-T-06	LDAP-API
O-T-07	Zuweisung von Berechtigungen ausschließlich über die Zuweisung von Rollen
O-T-08	Softwaremodul / Komponente / Funktion für Rollen- und Berechtigungsmanagement

Organisatorische Maßnahmen	
O-O-05	Formalisiertes und dokumentiertes Rollen- und Berechtigungskonzept

8.4 Updates und Patches

Adressiertes Risiko Wenn sicherheitsrelevante Updates und Patches nicht sofort nach ihrer Veröffentlichung installiert werden, könnten Angreifer die durch das Update oder Patch behobene Schwachstelle rekonstruieren und aktiv ausnutzen.

Ziel Die Zeit zwischen der Veröffentlichung von Updates und Patches, ihrer Bereitstellung für BASF und ihrer Installation ist so kurz, dass es für Angreifer unmöglich ist, bekannte, noch nicht behobene Schwachstellen aktiv auszunutzen.

Technische Maßnahmen	
O-T-09	Bereitstellung von sicherheitsrelevanten Updates und Patches innerhalb der Lösung
O-T-10	Bereitstellung von sicherheitsrelevanten Updates und Patches über die Website des Anbieters

Organisatorische Maßnahmen	
O-O-06	Informationen über neu veröffentlichte Updates und Patches per E-Mail
O-O-07	Informationen über neu veröffentlichte Updates und Patches innerhalb der Lösung
O-O-08	Informationen über neu veröffentlichte Updates und Patches auf der Website des Anbieters

8.5 Penetrationstests

Adressiertes Risiko Die Komplexität von Lösungen kann dazu führen, dass Schwachstellen aufgrund der Interaktion von Teilkomponenten und der daraus resultierenden Auswirkungen unbemerkt bleiben. Solche blinden Flecken könnten von Angreifern ausgenutzt werden.

Ziel Das Schutzniveau der Gesamtlösung wird regelmäßig unter Berücksichtigung aller bekannten Angriffsmethoden überprüft und auf Basis der Erkenntnisse weiterentwickelt.

Organisatorische Maßnahmen

O-O-09	Regelmäßige Penetrationstests der Lösung
O-O-10	Ereignisgesteuerte Penetrationstests der Lösung, z. B. bei wesentlichen Änderungen
O-O-11	Regelmäßige Penetrationstests von Fremdkomponenten, z.B. Softwaremodule von externen Entwicklern
O-O-12	Ereignisgesteuerte Penetrationstests von Komponenten Dritter, z. B. wenn Sicherheitslücken oder Sicherheitsvorfälle festgestellt werden

8.6 Unterstützung und Dokumentation für Benutzer

Adressiertes Risiko Fehlende oder nicht verfügbare Gebrauchsanweisungen könnten dazu führen, dass die Anwender die Lösung nicht oder falsch verwenden. Dies könnte sich nachteilig auf den Betrieb der BASF auswirken.

Ziel Alle Benutzergruppen sind in der Lage, die Lösung in der vorgesehenen Weise und für den vorgesehenen Zweck zu nutzen.

Technische Maßnahmen

O-T-11	Community-Forum für den Austausch zwischen Nutzern
O-T-12	Helpdesk-Website für Benutzer
O-T-13	Telefon-Hotline für Nutzer
O-T-14	Unterstützung per E-Mail für Benutzer

Organisatorische Maßnahmen

O-O-13	Schulungsangebote für Nutzer(gruppen) durch eigene Ausbilder des Anbieters
O-O-14	Schulungsangebote für Nutzer(gruppen) durch externe Schulungsanbieter, z. B. Industrieverbände, TÜV

O-O-15	Selbstlernmaterialien für Nutzer(gruppen), z. B. Lernvideos, Präsentationen, Schritt-für-Schritt-Anleitungen
O-O-16	Allgemeine Benutzerhandbücher
O-O-17	Szenario basierte Benutzerhandbücher

8.7 Unterstützung und Dokumentation für Administratoren

Adressiertes Risiko Eine unsachgemäße Installation, Verteilung oder Konfiguration könnte zu kompromittierten Daten oder einem Ausfall der Lösung führen und damit den Betrieb der BASF stören.

Ziel BASF-Administratoren, die für den Betrieb der Lösung verantwortlich sind, werden in die Lage versetzt, die Lösung wie vorgesehen zu verwalten.

Technische Maßnahmen	
O-T-15	Community-Forum für den Austausch zwischen Administratoren
O-T-16	Helpdesk-Website für Administratoren
O-T-17	Telefon-Hotline für Administratoren
O-T-18	Unterstützung per E-Mail für Administratoren

Organisatorische Maßnahmen	
O-O-18	Schulungen für Administratoren durch die eigenen Ausbilder des Anbieters
O-O-19	Schulungsangebote für Administratoren durch externe Schulungsanbieter, z. B. Industrieverbände, TÜV
O-O-20	Selbstlernmaterialien für Administratoren, z. B. Lernvideos, Präsentationen, Schritt-für-Schritt-Anleitungen
O-O-21	Allgemeine Handbücher für Administratoren
O-O-22	Szenario basierte Handbücher für Administratoren

8.8 Software-Architektur

Adressiertes Risiko Wenn ein Zugriff von außerhalb der BASF-Infrastruktur über das Internet möglich ist, könnten Angreifer funktionale und architektonische Schwachstellen ausnutzen, um Daten abzurufen oder im Falle eines erfolgreichen Angriffs über eine Erweiterung der Privilegien Zugriff auf andere Systeme innerhalb der BASF-Infrastruktur zu erhalten.

Ziel Sowohl die Architektur als auch die Prozesse zur Datenverarbeitung sind so ausgelegt, dass die Lösung und die verarbeiteten Daten vor unberechtigtem Zugriff geschützt sind und bei einer Kompromittierung einzelner Komponenten keine anderen BASF-Systeme betroffen sind.

Technische Maßnahmen	
O-T-19	3-Tier-Architektur: Trennung von Darstellungs-, Verarbeitungs- und Datenspeicherungsebene
O-T-20	2-Tier-Architektur: Trennung von Anwendungs- und Datenspeicherebene
O-T-21	Schutz vor Cross-Site-Scripting
O-T-22	Eingabevalidierung zum Schutz vor unbefugter Datenmanipulation, z. B. durch SQL-Injection

Organisatorische Maßnahmen	
O-O-23	Dokumentation der Architektur der Lösung

9 Cloud-Lösungen

Beschaffung von Anwendungen (Paketen), die auf der Infrastruktur eines Dienstanbieters betrieben werden und deren Nutzung zwingend einen Internetzugang voraussetzt. Dabei ist es unerheblich, ob es sich um eine SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service), Iaas (Infrastructure-as-a-Service) oder eine hier nicht spezifische Cloud-Technologie handelt.

9.1 IT-Sicherheitskonzept

Adressiertes Risiko Werden branchenübliche Sicherheitsmechanismen bei der Planung und Entwicklung nicht berücksichtigt oder die Wechselwirkungen zwischen den Maßnahmen nicht erkannt, könnten Angreifer die daraus resultierenden Schwachstellen ausnutzen und die Informationen, Daten und Infrastruktur der BASF kompromittieren.

Ziel Im Rahmen eines IT-Sicherheitskonzepts wird die Gesamtheit aller Sicherheitsmaßnahmen für eine Lösung definiert und der Umsetzungsstand kontinuierlich dokumentiert und bei Änderungen aktualisiert.

Organisatorische Maßnahmen	
CL-O-01	Entwicklung eines IT-Sicherheitskonzepts für die Lösung
CL-O-02	Regelmäßige Aktualisierung des IT-Sicherheitskonzepts und bei Änderungen
CL-O-03	Bereitstellung einer Dokumentation der implementierten Sicherheitsmechanismen für BASF

9.2 Kryptographie

Angesprochenes Risiko Wenn Daten während der Speicherung, Verarbeitung oder Übertragung nicht geschützt sind, könnten sie von unbefugten Dritten abgefangen oder kompromittiert werden.

Ziel Während des gesamten Lebenszyklus sind die Daten vor unbefugtem Zugriff geschützt.

Technische Maßnahmen	
CL-T-01	Verschlüsselung von Daten während der Übertragung (Data at Transit), z. B. HTTPS, SSH
CL-T-02	Verschlüsselung von Daten während der Speicherung, z. B. Datenbankverschlüsselung
CL-T-03	Multi-Faktor-Authentifizierung für den Zugriff auf sensible Informationen
CL-T-04	Multi-Faktor-Authentifizierung für Konfigurationsänderungen

Organisatorische Maßnahmen	
CL-O-04	Krypto-Konzept mit allen implementierten Verschlüsselungsmethoden und Schlüssellängen

9.3 Rollen und Berechtigungskonzept

Adressiertes Risiko Ein fehlendes oder unzureichendes Rollen- und Berechtigungskonzept könnte es unbefugten Benutzern ermöglichen, Zugang zu sensiblen Informationen zu erhalten.

Ziel Rollen und Berechtigungen können granular verwaltet werden, so dass die Benutzer nur auf die Informationen zugreifen können, die sie zur Erfüllung ihrer Aufgaben benötigen.

Technische Maßnahmen	
CL-T-05	Active-Directory-API
CL-T-06	LDAP-API
CL-T-07	Zuweisung von Berechtigungen ausschließlich über die Zuweisung von Rollen
CL-T-08	Softwaremodul / Komponente / Funktion für Rollen- und Berechtigungsmanagement

Organisatorische Maßnahmen	
CL-O-05	Formalisiertes und dokumentiertes Rollen- und Berechtigungskonzept

9.4 Schutz vor Malware

Adressiertes Risiko Wenn Systeme kompromittiert werden, könnten Informationen unbeabsichtigt verändert oder unbefugten Dritten zugänglich gemacht werden.

Ziel Es wird sichergestellt, dass keine Schadsoftware auf IT-Geräten installiert werden kann.

Technische Maßnahmen	
CL-T-09	Lösung zum Schutz vor Malware für Server
CL-T-10	Lösung zum Schutz vor Malware auf den Clients, z. B. Microsoft Defender
CL-T-11	Sicherheitsanwendungen, z. B. Firewall, SIEM
CL-T-12	Geeignete Segmentierung des Unternehmensnetzes auf der Grundlage der Kritikalität der Anforderungen an die Vertraulichkeit und Verfügbarkeit der verarbeiteten Daten
CL-T-13	Verwendung einer Sandbox-Lösung zum Öffnen unbekannter Dateien oder Dateien von unbekannten Absendern.
CL-T-14	Zentral verwaltete Softwareverteilung
CL-T-15	Keine Vergabe von lokalen Administratorrechten an Benutzer
CL-T-16	Keine Vergabe von lokalen Administratorrechten an Entwickler

Organisatorische Maßnahmen	
CL-O-06	Prozess zur sofortigen Installation von sicherheitsrelevanten Updates aller eingesetzten Softwarelösungen
CL-O-07	Härtungsrichtlinie für Server
CL-O-08	Härtungsrichtlinie für Clients
CL-O-09	Härtungsrichtlinie für Smartphones

9.5 Datensicherung

Adressiertes Risiko Systemfehler, Schadsoftware oder Missbrauch von IT-Systemen könnten zum Verlust von Daten führen.

Ziel Alle für die BASF relevanten Daten werden regelmäßig gesichert und können im Falle eines Datenverlustes wiederhergestellt werden.

Technische Maßnahmen	
CL-T-17	Regelmäßige, automatisierte Sicherung aller für die BASF relevanten Daten
CL-T-18	Automatisierter Arbeitsablauf für die Bereitstellung, z. B. CI/CD

Organisatorische Maßnahmen	
CL-O-10	Datensicherungskonzept
CL-O-11	Regelmäßige Übungen zur Datensicherung und -wiederherstellung
CL-O-12	Manuelle Snapshots der Systemzustände vor jeder signifikanten Änderung an den Systemen und Anwendungen, die für die Ausführung der Lösung erforderlich sind

9.6 Penetrationstests

Adressiertes Risiko Die Komplexität von Lösungen kann dazu führen, dass Schwachstellen aufgrund der Interaktion von Teilkomponenten und der daraus resultierenden Auswirkungen unbemerkt bleiben. Solche blinden Flecken könnten von Angreifern ausgenutzt werden.

Ziel Das Schutzniveau der Gesamtlösung wird regelmäßig unter Berücksichtigung aller bekannten Angriffsmethoden überprüft und auf Basis der Erkenntnisse weiterentwickelt.

Organisatorische Maßnahmen	
CL-O-13	Regelmäßige Penetrationstests der Lösung
CL-O-14	Ereignisgesteuerte Penetrationstests der Lösung, z. B. bei wesentlichen Änderungen
CL-O-15	Regelmäßige Penetrationstests von Fremdkomponenten, z.B. Softwaremodule von externen Entwicklern
CL-O-16	Ereignisgesteuerte Penetrationstests von Komponenten Dritter, z. B. wenn Sicherheitslücken oder Sicherheitsvorfälle festgestellt werden

9.7 Unterstützung und Dokumentation für Benutzer

Adressiertes Risiko Fehlende oder nicht verfügbare Gebrauchsanweisungen könnten dazu führen, dass die Anwender die Lösung nicht oder falsch verwenden. Dies könnte sich nachteilig auf den Betrieb der BASF auswirken.

Ziel Alle Benutzergruppen sind in der Lage, die Lösung in der vorgesehenen Weise und für den vorgesehenen Zweck zu nutzen.

Technische Maßnahmen	
CL-T-19	Community-Forum für den Austausch zwischen Nutzern
CL-T-20	Helpdesk-Website für Benutzer
CL-T-21	Telefon-Hotline für Nutzer
CL-T-22	Unterstützung per E-Mail für Benutzer

Organisatorische Maßnahmen

CL-O-17	Schulungsangebote für Nutzer(gruppen) durch eigene Ausbilder des Anbieters
CL-O-18	Schulungsangebote für Nutzer(gruppen) durch externe Schulungsanbieter, z. B. Industrieverbände, TÜV
CL-O-19	Selbstlernmaterialien für Nutzer(gruppen), z. B. Lernvideos, Präsentationen, Schritt-für-Schritt-Anleitungen
CL-O-20	Allgemeine Benutzerhandbücher
CL-O-21	Szenario basierte Benutzerhandbücher

9.8 Unterstützung und Dokumentation für Administratoren

Adressiertes Risiko Eine unsachgemäße Installation, Verteilung oder Konfiguration könnte zu kompromittierten Daten oder einem Ausfall der Lösung führen und damit den Betrieb der BASF stören.

Ziel Die für den Betrieb der Lösung zuständigen BASF-Administratoren werden in die Lage versetzt, die Lösung wie vorgesehen zu verwalten.

Technische Maßnahmen

CL-T-23	Community-Forum für den Austausch zwischen Administratoren
CL-T-24	Helpdesk-Website für Administratoren
CL-T-25	Telefon-Hotline für Administratoren
CL-T-26	Unterstützung per E-Mail für Administratoren

Organisatorische Maßnahmen

CL-O-22	Schulungen für Administratoren durch die eigenen Ausbilder des Anbieters
CL-O-23	Schulungsangebote für Administratoren durch externe Schulungsanbieter, z. B. Industrieverbände, TÜV
CL-O-24	Selbstlernmaterialien für Administratoren, z. B. Lernvideos, Präsentationen, Schritt-für-Schritt-Anleitungen
CL-O-25	Allgemeine Handbücher für Administratoren
CL-O-26	Szenario basierte Handbücher für Administratoren

9.9 Software-Architektur

Adressiertes Risiko Angreifer könnten Schwachstellen in der Software-Architektur ausnutzen, um Daten abzurufen oder im Falle erfolgreicher Angriffe über eine Erweiterung der Privilegien Zugang zu anderen Systemen innerhalb der BASF-Infrastruktur zu erlangen.

Ziel Die Software-Architektur soll die Lösung und die verarbeiteten Daten vor unberechtigtem Zugriff schützen und sicherstellen, dass bei einer Kompromittierung einzelner Komponenten keine anderen BASF-Systeme betroffen sind.

Technische Maßnahmen

CL-T-27	3-Tier-Architektur: Trennung von Darstellungs-, Verarbeitungs- und Datenspeicherungsebene
CL-T-28	2-Tier-Architektur: Trennung von Anwendungs- und Datenspeicherebene
CL-T-29	Schutz vor Cross-Site-Scripting
CL-T-30	Eingabevalidierung zum Schutz vor unbefugter Datenmanipulation, z. B. durch SQL-Injection

Organisatorische Maßnahmen

CL-O-27	Dokumentation der Architektur der Lösung

9.10 Management der Geschäftskontinuität

Adressiertes Risiko Der Ausfall oder die Störung kritischer Systemkomponenten kann zu Einbußen bei der Verfügbarkeit von Cloud-Lösungen führen. Insbesondere bei kritischen Geschäftsprozessen kann bereits ein kurzer Ausfall zu einem erheblichen Schaden für BASF führen.

Ziel Die Einhaltung der vereinbarten Service Level Agreements (SLAs) kann über die gesamte Vertragslaufzeit gewährleistet werden.

Technische Maßnahmen	
CL-T-31	Notfall-Rechenzentrum
Organisatorische Maßnahmen	
CL-O-28	Benennung einer verantwortlichen Person für das Notfallmanagement, z. B. BCM-Beauftragter, Notfallbeauftragter
CL-O-29	Management der Gesamtheit aller Notfallmanagementmaßnahmen im Rahmen eines Business Continuity Management Systems (BCMS)
CL-O-30	Redundanzkonzept

9.11 Schutz persönlicher Informationen (PII)

Angesprochenes Risiko Bei der Verarbeitung personenbezogener Daten im Rahmen der Auftragsverarbeitung könnten die Persönlichkeitsrechte der betroffenen Personen durch eine unsachgemäße Verwendung der Informationen beeinträchtigt werden.

Ziel Bei der Verarbeitung von PII wird jederzeit sichergestellt, dass die Anforderungen der DSGVO und nachgelagerter Datenschutzbestimmungen eingehalten werden.

Organisatorische Maßnahmen	
CL-O-31	Benennung einer für den Datenschutz verantwortlichen Person, z. B. eines Datenschutzbeauftragten
CL-O-32	Schutz der Gesamtheit aller personenbezogenen Daten im Rahmen eines Datenschutzmanagementsystems (DMS)

9.12 Physische Sicherheit

Adressiertes Risiko Wenn Cloud-Lösungen in ungesicherten Rechenzentren betrieben werden, können Server und andere IT-Komponenten manipuliert, gestohlen oder zerstört werden.

Ziel Die gesamte für die Bereitstellung der Cloud-Lösung erforderliche Infrastruktur wird in einem sicheren Rechenzentrum betrieben.

Technische Maßnahmen	
CL-T-32	Feuerlösch- und Brandschutzsystem
CL-T-33	Mehrere Brandabschnitte
CL-T-34	Gefahrenmeldeanlage
CL-T-35	Videoüberwachungssystem
CL-T-36	Automatisierte Überwachung der Infrastruktur
CL-T-37	Anbindung des Rechenzentrums an einen zentralen, rund um die Uhr besetzten Leitstand
CL-T-38	Temperatur- und Feuchtigkeitsmanagement
CL-T-39	Unterbrechungsfreie Stromversorgung
CL-T-40	Überspannungsschutzgerät

Organisatorische Maßnahmen

CL-O-33	Maßnahmen zum Schutz vor Staub
CL-O-34	Konzept der Zugangskontrolle

10 Software-Entwicklung

Entwicklung von Softwarelösungen oder -komponenten, die eigenständig oder in Verbindung mit anderen Lösungen verwendet werden. Dazu gehört auch die Anpassung von Lösungen. Die Konfiguration einer Lösung fällt nicht unter Softwareentwicklung.

Hinweis zur Anwendung: Die Anforderungen an die Softwareentwicklung sind zusätzlich zu den Leistungstypen On-Premise Solutions und Cloud Solutions zu erfüllen, wenn Anbieter selbst Lösungen entwickeln.

10.1 Entwicklungsprozess

Adressiertes Risiko Wenn bewährte Verfahren für die sichere Softwareentwicklung nicht angewandt werden, kann dies zu Sicherheitslücken führen, die von Angreifern ausgenutzt werden könnten. Dies gilt sowohl für den Quellcode als auch für die Konfiguration der bereitgestellten Installationsmedien.

Ziel Ein standardisierter und verwalteter Entwicklungsprozess stellt sicher, dass alle bekannten Sicherheitslücken in der verwendeten Software (Pakete) geschlossen und die Installationsmedien vor der Bereitstellung ausreichend sicher konfiguriert werden.

Technische Maßnahmen	
SW-T-01	Automatisiertes Deployment von Software, z. B. CI/CD
Organisatorische Maßnahmen	
SW-O-01	Formalisierter Lebenszyklus für sichere Softwareentwicklung (SSDLC)
SW-O-02	Verwaltung und Dokumentation der im Entwicklungsprozess verwendeten Werkzeuge
SW-O-03	Testen neuer Versionen der Software auf der Grundlage standardisierter Testfälle
SW-O-04	Durchführung von Einheitstests
SW-O-05	Durchführung von Belastungstests
SW-O-06	Einhaltung des Grundsatzes: Security by Design
SW-O-07	Einhaltung des Grundsatzes: Security by Default

SW-O-08	Einhaltung des Grundsatzes: Privacy by Design
SW-O-09	Einhaltung des Grundsatzes: Privacy by Default

10.2 Software von Drittanbietern

Angesprochenes Risiko Bei der Verwendung von Softwarekomponenten von Drittanbietern, wie z. B. Softwaremodulen von externen Entwicklern, können Schwachstellen in diesen Komponenten Angreifern als Angriffsvektoren dienen, um unbefugten Zugriff auf Daten zu erhalten.

Ziel Alle Softwarekomponenten von Drittanbietern werden regelmäßig auf Schwachstellen überprüft. Sicherheitsrelevante Updates und Patches von Fremdkomponenten werden vom Lieferanten über den für die Lösung vereinbarten allgemeinen Update- und Patch-Kanal bereitgestellt.

Organisatorische Maßnahmen	
SW-O-10	Register aller Softwarekomponenten von Drittanbietern
SW-O-11	Regelmäßiges Prüfverfahren für bekannte Schwachstellen der verwendeten Softwarekomponenten von Drittanbietern.