Informationssicherheitsvorgaben

Lieferanten (mit IT-Betrieb)

OA1002-05

group24 AG (group24)

INHALTSVERZEICHNIS

STAMMDATEN

Referenz-Nummer:	OA1002-05
Dokumententitel:	Informationssicherheitsrichtlinie Lieferanten
Fachlich Verantwortlicher:	Roman Dummel
Zuständiger Bereich:	IT-Consulting
Geltungsbereich:	group24 AG
Gültig von:	01.11.2022
Gültig bis:	31.12.2024
Verantwortlicher Prüfer:	Andreas Badry
Wiedervorlage Datum:	01.10.2024
Dokumentenkategorie	Intern

ÄNDERUNGSVERZEICHNIS

Version	Datum	Autor	Inhalte der Änderung
0.1	22.06.2022	Sandra Kiemes (extern)	Initiale Erstellung
0.2	22.12.2022	Roman Dummel	Anpassung auf die group24

REVIEWNACHWEIS UND FREIGABE

Version	Datum	Teilnehmer	Inhalte des Reviews
V1.0	23.12.2022	Andreas Badry	Prüfung Ersterstellung und Freigabe
V1.1	30.11.2023	Andreas Badry	Review 2023

1 EINFÜHRUNG UND GELTUNGSBEREICH

1.1 Einleitung

In dieser Richtlinie werden Regeln für den Umgang mit Informationen und den Einsatz von Informationstechnik definiert, die Lieferanten, Werkunternehmer und Dienstleister - nachfolgend Auftragnehmer genannt - der Group24 AG– nachfolgend group24 genannt - zu befolgen haben. Zweck dieser Richtlinie ist der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der Rechte und Interessen des Auftraggebers sowie aller natürlichen und juristischen Personen, die eine Geschäftsbeziehung mit group24 eingehen und / oder Tätigkeiten für diesen ausführen.

1.2 Geltungsbereich

Diese Richtlinie richtet sich an die Geschäftsleitung des Auftragnehmers, deren Mitarbeiter sowie deren Erfüllungs- /Verrichtungsgehilfen.

2 WAHRUNG VON VERTRAULICHKEIT VON INFORMATIONEN/BETRIEBSGEHEIMNISSEN

Group24 arbeitet ausschließlich mit Auftragnehmern zusammen, welche sich zur Wahrung von Vertraulichkeit von Informationen und Betriebsgeheimnissen im Rahmen einer Geheimhaltungsverpflichtung oder einer Geheimhaltungsvereinbarung verpflichtet haben. In Einzelfällen, wenn die übergebenen Informationen einem gesteigerten Sicherheitsbedürfnis unterfallen, können darüber hinaus besondere Maßnahmen von Auftragnehmern gefordert werden, um dem gesteigerten Sicherheitsbedürfnis Rechnung zu tragen. Bspw. kann dem Auftragnehmer untersagt werden, ohne Zustimmung von Group24 übermittelte Informationen an Dritte weiter zu geben, zu bearbeiten oder zu speichern. Eine Zustimmung kann an die Einhaltung der nachfolgenden Sicherheitsanforderungen beim Auftragnehmer oder seinen Subunternehmern geknüpft werden.

3 ANFORDERUNGEN AN AUFTRAGNEHMER ZUR AUFRECHTERHALTUNG DER INFORMATIONSSICHERHEIT

3.1 Grundsätzliches

Die Group24 empfiehlt jedem Auftragnehmer mit datenschutzrechtlicher bzw. informationssicherheitstechnischer Relevanz ein Managementsystem für den Datenschutz bzw. die Informationssicherheit umzusetzen. Als Grundlage sollten anerkannte Standards wie z. B. die ISO 27001 dienen. Die Notwendigkeit eines solchen Managementsystems ist jedoch nicht verbindlich, sofern nicht explizit durch die Group24 eingefordert.

In Abhängigkeit der Form der Zusammenarbeit ergeben sich Schwerpunkte bei den Anforderungen der umzusetzenden Sicherheitsmaßnahmen. Im Laufe der Geschäftsbeziehung kann sich die Form der Zusammenarbeit ändern. In diesem Zusammenhang ändern sich auch die umzusetzenden Sicherheitsmaßnahmen.

3.2 Organisation der Informationssicherheit

Es sind Richtlinien, Prozesse und Verantwortlichkeiten zu definieren, mit denen die Informationssicherheit implementiert und kontrolliert werden kann.

Dies beinhaltet insbesondere:

- Die Erstellung einer Informationssicherheitsrichtlinie.
- Anwenderrichtlinien zur Festlegung von Regeln für den Umgang mit Anwendungen, Systemen und IT-Endgeräten und dem Verhalten bei der Nutzung von Informationstechnologie.
- Die Beschreibung von Prozessen für die Verwaltung von Datenträgern, Dokumenten und Informationen.
- Die Festlegung der Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit.
- Die Verpflichtung der Mitarbeiter auf Geheimhaltung und Wahrung des Datengeheimnisses.
- Die regelmäßige Durchführung von Schulungen und Awareness-Maßnahmen.

3.3 Zugriffskontrolle

Umsetzung von Maßnahmen, die gewährleisten, dass die zur Benutzung der Informationsverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten bzw. schutzbedürftigen Informationen und Daten zugreifen können.

Dies beinhaltet insbesondere folgende Maßnahmen:

- Die Erstellung von Berechtigungskonzepten für den Zugriff auf schützenswerte Informationen, Systeme und Applikationen.
- Die Umsetzung von Zugriffsbeschränkungen.
- Die Vermeidung der Konzentration von Funktionen und Etablieren einer Funktionstrennung.
- Die Umsetzung eines Prozesses zur Berechtigungsvergabe.
- Die regelmäßige Überprüfung der Berechtigungen.
- Die Protokollierung der Berechtigungsvergabe und des Datenzugriffs.

3.4 Kryptographie

Der Einsatz von Verschlüsselungsverfahren für die Sicherstellung des ordnungsgemäßen und wirksamen Schutzes der Vertraulichkeit, Authentizität oder Integrität von personenbezogenen Daten bzw. schutzbedürftigen Informationen.

Dies beinhaltet insbesondere:

- Die Verschlüsselung von Datenträgern und Festplatten von PC, Laptops, Verzeichnissen.
- Die gesicherte Speicherung von Daten auf mobilen Datenträgern. Als vertrauliche oder geheim klassifizierte Daten sind auf mobilen Datenträgern zu verschlüsseln.

3.5 Schutz von Gebäuden

Umsetzung von Maßnahmen, die den unautorisierten physischen Zugriff auf die Informationen und informationsverarbeitende Einrichtungen der Organisation sowie deren Beschädigung und Beeinträchtigung verhindern.

Alle Lieferanten müssen sicherstellen, dass der Zugang zu unseren Systemen und Daten nur autorisierten Personen gewährt wird. Dazu müssen angemessene Zugangskontrollen wie Passwörter, Zugriffsbeschränkungen und

Sicherheitsprüfungen eingerichtet werden. Alle Zugriffe auf unsere Systeme und Daten müssen protokolliert werden.

3.6 Schutz von Betriebsmitteln / Informationswerten

Es sind geeignete Schutzmaßnahmen zur Vorbeugung von Verlust, Beschädigung, Diebstahl oder Beeinträchtigung von Betriebsmitteln / Informationswerten und zur Vermeidung von Unterbrechungen der Betriebstätigkeit der Organisation zu implementieren.

Dies beinhaltet insbesondere:

- Regelungen zur sicheren Platzierung von Betriebsmitteln.
- Schutz der Betriebsmittel vor Überspannung, Stromausfall, Wasser und Feuer.
- Schutz von Informationen und Systeme der Informationsverarbeitung vor Diebstahl.
- Regelungen zur regelmäßigen Wartung von Betriebsmitteln.
- Die Implementierung eines Prozesses zur sicheren Löschung, Entsorgung und Vernichtung von Betriebsmitteln.

3.7 Betriebsverfahren und Zuständigkeiten

Es ist der ordnungsgemäße und sichere Betrieb von Systemen und Verfahren zur Verarbeitung von Informationen sicherzustellen.

Dies beinhaltet insbesondere:

- Die Dokumentation der Betriebsverfahren, z.B. in Form von Betriebsführungshandbüchern.
- Die Härtung der IT-Systeme.
- Die getrennte Verarbeitung von Produktiv- und Testdaten.
- Die Sicherstellung der Mandantentrennung / Mandantenfähigkeit.
- Die Anforderungen einer Funktionstrennung sind umzusetzen. Es ist festzulegen, zu dokumentieren und zu begründen, welche Funktionen nicht miteinander vereinbar sind, also nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Grundsätzlich sind dabei operative Funktionen nicht mit kontrollierenden Funktionen vereinbar.

3.8 Datensicherungen

Es sind Maßnahmen umzusetzen, die gewährleisten, dass schutzbedürftige Informationen und Daten / personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Dies beinhaltet insbesondere:

- Die Erstellung eines Datensicherungskonzeptes.
- Die regelmäßige Durchführung von Datensicherungen.
- Die Datensicherungsmedien sind getrennt von den produktiven Systemen aufzubewahren.

3.9 Schutz vor Malware durch Schwachstellen- und Patchmanagement

Eine Ausnutzung technischer Schwachstellen sind durch den Einsatz von aktueller Virenschutzsoftware und die Implementierung eines Patchmanagements zu verhindern.

Es sind regelmäßige Überprüfungen zur Erkennung von Schwachstellen durchzuführen.

3.10 Protokollierung und Überwachung

Es sind Maßnahmen zu implementieren, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem (personenbezogene) Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind.

Dies beinhaltet insbesondere folgende Maßnahmen:

- Die Protokollierung der Berechtigungsvergabe und des Datenzugriffs.
- Die regelmäßige Überprüfung von Benutzerberechtigungen.
- Die Protokollierung der Aktivitäten und regelmäßige Auswertung der Benutzer- und Systemaktivitäten

3.11 Netzwerksicherheitsmanagement

Es muss ein angemessener Schutz für das Netzwerk implementiert werden, so dass die Informationen und die Infrastrukturkomponenten geschützt werden.

Dies beinhaltet insbesondere:

- Die Implementierung eines Netzwerkmanagements.
- Die Umsetzung einer Benutzerauthentifizierung für externe Verbindungen und Verbindungen zwischen einzelnen Systemen.
- Die Gewährleistung eines Schutzes der Diagnose- und Konfigurationsports.
- Sicherheitsgateways an den Übergabepunkten / Netzgrenzen.
- Die Isolation sensitiver Systeme.

3.12 Informationsübertragung

Es sind Maßnahmen zu implementieren, die gewährleisten, dass personenbezogene Daten bzw. schutzbedürftige Informationen und Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten bzw. schutzbedürftiger Informationen und Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. (Beschreibung der verwendeten Einrichtungen und Übermittlungsprotokolle, z.B. Identifizierung und Authentifizierung, Verschlüsselung entsprechend dem Stand der Technik, automatischer Rückruf, u.a.)

Dies beinhaltet insbesondere:

- Den sicheren Transport und den Versand von Daten / Dokumenten in Abhängigkeit vom Schutzbedarf der Daten.
- Den Abschluss von Verträgen zum Schutz von Geschäftsgeheimnissen mit Dritten und Unterlieferanten.
- Die Protokollierung der Datenübertragungen.
- Die Beschreibung von Schnittstellen zwischen Systemen und der externen Datenverbindungen

3.13 Netztrennung

Gruppen von Informationsdiensten, Mandanten, Benutzern und Informationssystemen sollten in Netzwerken voneinander getrennt gehalten werden.

Dies beinhaltet insbesondere:

- Gruppen von Informationsdiensten, Mandanten, Benutzern und Informationssystemen sollten in Netzwerken voneinander getrennt gehalten werden.
- Um das Risiko zu mindern, dass personenbezogene Daten bzw. schutzbedürftige Informationen und Daten, die zwischen IT-Systemen weitergegeben werden, auf dem Netz mitgelesen werden, sind diese zu segmentieren.
- Direkte Verbindungen des Clients zum Internet sind bei remote Zugriffen (z.B. über VPN oder RAS) auf das Unternehmensnetz durch geeignete Maßnahmen zu unterbinden.

3.14 Anschaffung, Entwicklung und Instandhaltung von Systemen

Es sind Maßnahmen und Prozesse zu implementieren, die sicherstellen, dass Informationssicherheit ein fester Bestandteil über den Lebenszyklus von Informationssystemen ist.

Dies beinhaltet insbesondere:

- Die Festlegung von sicherheitsspezifischen Regelungen und Anforderungen für den Einsatz neuer Informationssysteme und für die Erweiterung bestehender Informationssysteme.
- Die Festlegung von Regelungen für die Entwicklung und Anpassung von Software und Systemen.
- Die Entwicklung von Leitlinien zur sicheren Systementwicklung.
- Die Überwachung von ausgelagerten Systementwicklungstätigkeiten.
- Der Schutz von Testdaten.

3.15 Lieferantenbeziehungen

Die umzusetzenden Sicherheitsmaßnahmen zur Verringerung von Risiken im Zusammenhang mit dem Einsatz von Externen sollten mit Sublieferanten / Subunternehmern vereinbart und dokumentiert werden.

Dies beinhaltet insbesondere:

- Die schriftliche Adressierung von Sicherheitsthemen in Verträgen mit Sublieferanten
- Die Überprüfung der Sicherheit bei Subunternehmern

3.16 Management von Informationssicherheitsvorfällen

Es sind konsistente und wirksame Maßnahmen für das Management von Informationssicherheitsvorfällen (Diebstahl, Systemausfall, Datenverlust etc.) zu implementieren.

Dies beinhaltet insbesondere:

- Die unverzügliche Meldung von Informationssicherheitsvorfällen an den Auftraggeber.
- Die Protokollierung von Sicherheitsvorfällen.
- Die Implementierung von Prozessen zur Einleitung von Maßnahmen zur Verhinderung / Wiederholung von Informationssicherheitsvorfällen.

3.17 Informationssicherheitsaspekte des Business Continuity Management / Notfall Managements

Die Aufrechterhaltung der Systemverfügbarkeit in schwierigen Situationen wie Krisen- oder Schadensfällen muss aufrechterhalten werden. Ein Notfallmanagement muss dieses sicherstellen. Die Anforderungen bezüglich der Informationssicherheit sollten bei den Planungen zur Betriebskontinuität und Notfallwiederherstellung festgelegt werden.

Dies beinhaltet insbesondere:

- Die Schaffung von Redundanzen für kritische Komponenten.
- Die Risikoabschätzung und Planung von Maßnahmen zur Sicherstellung des Geschäftsbetriebes.
- Die Erstellung von Notfallplänen.
- Die regelmäßige Durchführung von Tests bzgl. der Wirksamkeit der Notfallmaßnahmen
- Frühzeitige Information des Auftraggebers bei Notfällen.

3.18 Einhaltung gesetzlicher und vertraglicher Anforderungen

Implementierung von Maßnahmen zur Vermeidung von Verstößen gegen gesetzliche, amtliche oder vertragliche Verpflichtungen sowie gegen jegliche Sicherheitsanforderungen.

Dies beinhaltet insbesondere:

- Den Abschluss von Geheimhaltungsverpflichtungen mit Mitarbeitern sowie Sublieferanten.
- Die Sicherstellung der Einhaltung der gesetzlichen Verpflichtungen im Rahmen der Zusammenarbeit.
- Die Rückgabe sämtlicher Daten, Betriebsmittel und Informationswerte an den Auftraggeber bei Vertragende.

3.19 Datenschutzanforderungen und Datenschutzmanagement

Die Privatsphäre sowie der Schutz von personenbezogenen Daten sollten entsprechend den Anforderungen der relevanten Gesetze, Vorschriften und ggf. Vertragsbestimmungen sichergestellt werden.

Dies beinhaltet insbesondere:

- Die Einhaltung der gesetzlichen Anforderungen im Rahmen der Auftragsdatenverarbeitung.
- Die unverzügliche Meldung von Datenschutzvorfällen an den Auftraggeber.

3.20 Informationssicherheitsüberprüfungen

Es muss regelmäßig überprüft werden, ob die Informationsverarbeitung entsprechend der definierten Sicherheitsmaßnahmen durchgeführt wird. Hierfür wird der Auftragnehmer regelmäßige Prüfungen durchführen. Der Auftragnehmer räumt dem Auftraggeber das Recht ein, regelmäßige Prüfungen beim Auftragnehmer durchzuführen.

4 ÜBERPRÜFUNG DER UMSETZUNG VON SICHERHEITSMAßNAHMEN

Group24 behält sich das Recht vor die Umsetzung der in Kapitel 3 dargestellten Sicherheits- Anforderungen zu überprüfen.