A03-1_V1_GIZ-DSM-_ISM_Tool_Anlage Informationssicherheit

Die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH betreibt ein Informationssicherheits-Managementsystem (ISMS) und plant eine Zertifizierung gemäß ISO/IEC 27001 sowie die Aufrechterhaltung dieses Zertifikats. Im Rahmen der Zertifizierung wird die aktuelle Version des genannten Standards umgesetzt.

Folgende Regelungen zur Informationssicherheit finden bei der Leistungserbringung Anwendung:

1 Meldung von Sicherheitsvorfällen

Die AN informiert die AG (informationsecuritymanagement@giz.de) unverzüglich und in angemessener Form über Informationssicherheitsvorfälle, die (auch) Informationen der GIZ betreffen.

Ein Informationssicherheitsvorfall ist ein Ereignis, durch welches eine Beeinträchtigung der Informationssicherheit möglich oder bereits erfolgt ist, z.B. durch unberechtigte Einsichtnahme/Weitergabe von Informationen (Verlust der Vertraulichkeit), Modifikation von Informationen (Verlust der Integrität) oder Löschen von Informationen/Behinderung des Zugriffs auf Informationen (Verlust der Verfügbarkeit).

2 Aufbewahrung von GIZ-bezogenen Unterlagen, Vertragsende

Auftragsbezogene Unterlagen und Arbeitsergebnisse, einschließlich der finanziellen Dokumentation, sind von der AN zehn Jahre nach Abnahme des Schlussberichts bzw. der Werkleistung aufzubewahren. Auf Verlangen der AG sind diese zu übergeben.

Sonstige von der AG erhaltene Unterlagen, Hilfsmittel, Materialien oder Gegenstände, die der AN bestimmungsgemäß nicht dauerhaft überlassen wurden, hat der AN mit Vertragsende unverzüglich und unaufgefordert zu übergeben. Dies gilt auch für alle Kopien.

In den obengenannten Fällen hat die Übergabe in einem vom Auftraggeber definierten Verfahren zu erfolgen. Die Auftraggeberin ist auch berechtigt, ganz oder teilweise die sichere Löschung (d.h. nicht rekonstruierbar) oder Vernichtung zu verlangen. Die Löschung und das angewandte Löschverfahren sind der Auftraggeberin auf Verlangen z.B. durch eine schriftliche Erklärung nachzuweisen. Eine zusätzliche Vergütung erfolgt nicht.

Gesetzliche Aufbewahrungspflichten und -fristen bleiben von dieser Regelung unberührt.

3 Zugriff auf Informationen

Der Auftragnehmer darf ausschließlich auf die im Rahmen der Leistungserbringung spezifizierten Informationen analog oder über technische Zugänge zugreifen.

Der Zugriff auf davon abweichende Bereiche und Informationen ist untersagt.

Die Auftraggeberin legt bei Bedarf fest, wie der Auftragnehmer mit Metadaten umzugehen hat (unter Berücksichtigung des Vertraulichkeitsprinzips; Need-to-Know).

4 Nutzung von Endgeräten

Bei der Nutzung von Endgeräten im Rahmen der Auftragsdurchführung stellt die AN sicher, dass der Ort der Nutzung angemessen sicher ist und dass unbefugte Dritte diese nicht benutzen können. Es muss weiterhin sichergestellt werden, dass unbefugte Dritte keine GIZ-bezogenen Informationen einsehen können (z.B. über Blickschutzfolien).

5 Ort der Leistungserbringung

Die Leistung darf nicht außerhalb des Europäischen Wirtschaftsraums erbracht werden. Das Hosting der SaaS-Lösung muss auf dem Gebiet des Europäischen Wirtschaftsraum erfolgen.

Zugriff auf die SaaS-Lösung und die Daten der GIZ durch den Betreiber und Support-Dienstleister soll von einem Standort innerhalb des Europäischen Wirtschaftsraums.

6 Auditrecht

Während der gesamten Projektlaufzeit räumt der Auftragnehmer der Auftraggeberin das Recht zur Durchführung von Prüfungen hinsichtlich der Sicherheit der durch den Auftragnehmer verarbeiteten Informationen ein.

Die Prüfung findet soweit kein besonderer Anlass besteht grundsätzlich maximal einmal jährlich statt. Vor Beginn einer solchen Prüfung teilt der Auftraggeber den initialen Prüfungsgegenstand und den geplanten Umfang (mit einem angemessenen zeitlichen Vorlauf) mit, damit der Auftragnehmer entsprechend disponieren kann.

Im Rahmen der Leistungserbringung durch den Auftragnehmer hat die Auftraggeberin ein Auditrecht für die bereitgestellte Leistung inklusive der dazu notwendigen infrastrukturellen, organisatorischen, personellen und technischen Komponenten. Dieses Auditrecht kann auch durch von der Auftraggeberin beauftragte Dritte wahrgenommen werden.

Aufwände des Auftragnehmers zur Begleitung/Durchführung der Prüfungen der Aufraggeberin werden nicht gesondert vergolten.

7 Mindestanforderungen an Authentisierungsmittel/Passwörter

Der Auftragnehmer muss mindestens folgende Anforderungen an die Passwortqualität für alle Accounts, mit denen auf GIZ-Informationen zugegriffen wird/werden kann, umsetzen:

- Passwörter müssen mindestens 10 Zeichen lang sein, für privilegierte Konten mindestens 16 Zeichen
- Passwörter für technische Konten müssen mindestens 20 Zeichen lang sein, sofern ein regelmäßiger Passwortwechsel (z.B. über Managed Service Accounts) nicht gewährleistet werden kann
- Das Passwort muss sich aus 3 der 4 folgenden Merkmale zusammenzusetzen: Großbuchstaben (A bis Z), Kleinbuchstaben (a bis z), Ziffern (0 bis 9) und Sonderzeichen (zum Beispiel: !, $, #, %)
- Passwörter, die leicht zu erraten sind, dürfen nicht verwendet werden.
- Passwörter dürfen nicht identisch zu einem der letzten 10 benutzten Passwörter sein.
- Passwörter müssen regelmäßig geändert werden.

Für alle Benutzerkonten innerhalb der SaaS-Lösung muss eine Multi-Faktor-Authentifizierung (mindestens zwei Faktoren) genutzt werden, die den Azure-Regeln der GIZ folgt (gem. Leistungsbeschreibung, Kap. 2.1.4.1.7).

8 Zertifikatsfehler bei Nutzern

Es muss gewährleistet sein, dass bei der Nutzung von Zertifikaten, keine Zertifikatsfehler auftreten. Die Verantwortung für das entsprechende Monitoring liegt beim Auftragnehmer.

9 Mindestanforderungen an die Datensicherung

Aus der Datensicherung muss anhand folgender Punkte eine vollständige Wiederherstellung aller Daten und Funktionen möglich sein. Außerdem sind die Sicherungsintervalle, und akzeptierten Wiederherstellungszeiten einzuhalten:

- Ein Voll-Backup muss wöchentlich erstellt werden und mindestens 21 Tage aufbewahrt werden
- Ein Inkrementelles Backup muss täglich erstellt werden und bis zur Löschung des entsprechenden Vollbackups aufbewahrt werden
- RPO (akzeptabler Datenverlust) von maximal einem Arbeitstag
- RTO (akzeptable Wiederherstellung zur Betriebsfähigkeit) von maximal einem Arbeitstag
- Die technischen Komponenten und der Ort der Speicherung der Datensicherung müssen sich mindestens in zwei unterschiedlichen Brandabschnitten befinden.

10 Leistungskennzahlen

Für die Erbringung der Leistung und die Berichte werden folgende für die Informationssicherheit relevante Leistungskennzahlen vereinbart:

- Verfügbarkeit des Systems in 99,5% innerhalb der Betriebszeit (24/7/365)
- Verfügbarkeit des Services in 99,5% innerhalb der Servicezeit
- Reaktionszeit bei Störungen (Dienstleister): 4 Stunden
- Lösungszeit für sicherheitsrelevante Ereignisse: maximal 24 Stunden

Während der gesamten Vertragslaufzeit muss auf Anforderung der Auftraggeberin ein Bericht (maximal halbjährlich) zur Informationssicherheit zur Verfügung gestellt werden, über deren Inhalt sich Auftraggeberin und AN abstimmen. Bei Nichteinhaltung der beschriebenen Leistungskennzahlen kann die Auftraggeberin nach den gesetzlichen Regelungen Schadensersatz geltend machen oder die Vergütung mindern.

11 ISMS des Auftragnehmers

Der Auftragnehmer muss über ein angemessenes, dokumentiertes und implementiertes Informations-Sicherheits-Management-System (ISMS) verfügen, das dem Standard ISO/IEC 27001:2022 (bzw. aktuelle Folgeversionen) oder vergleichbar entspricht. Das ISMS muss die zu erbringende Leistung inklusive der verarbeitenden Informationen mit den dazu notwendigen infrastrukturellen, organisatorischen, personellen und technischen Komponenten umfassen.

Der Auftragnehmer muss eine/n Informationssicherheitsbeauftragte/n (Chief Information Security Officer) benennen, welche/r über die erforderliche Fachkunde verfügt und teilt der Auftraggeberin dessen/deren Kontaktdaten auf Anforderung mit.

Die Auftraggeberin wird einen Kontakt als ausschließliche/n Ansprechpartner/in in allen Fragen des Auftragnehmers bezüglich der Informationssicherheit benennen.

12 Benutzermanagement

Das ISMS des Auftragnehmers muss Verfahren zur dokumentierten Vergabe, Änderung, Sperrung, Entsperrung, Deaktivierung und Reaktivierung von (privilegierten, internen, externen und anderen) Benutzerkonten sowie zur zweifelsfreien Identifikation berechtigter Personen und zur Rücksetzung von Passwörtern beinhalten.

Diese Verfahren müssen technische Maßnahmen zum Schutz vor Brute-Force Angriffen (z.B. Sperrung von Benutzeraccounts nach mehrmaliger fehlerhafter Authentisierung) beinhalten.

Der Auftragnehmer muss im Rahmen seines ISMS für das Benutzermanagement folgendes sicherstellen:

- Benutzerkennungen müssen deaktiviert werden, wenn sie nicht mehr oder für mehr als 6 Monate nicht mehr benötigt werden.
- Benutzerkennungen dürfen nur gelöscht werden, wenn durch die Löschung keine Gefahr besteht, dass vorhandene Protokolle, Logdateien oder sonstige Aufzeichnungen innerhalb des Archivierungszeitraums nicht mehr eindeutig einer Person zugeordnet werden können.
- Werden nicht-personalisierte Benutzerkonten (z.B. root-Account, Benutzerkonten für den IT-Notfall) eingesetzt, so muss durch geeignete Maßnahmen sichergestellt werden, dass die mit diesem Konto durchgeführten Aktivitäten jederzeit zweifelsfrei einer handelnden bzw. verantwortlichen Person (möglichst automatisiert) zugeordnet werden können.
- Technische Benutzerkonten dürfen ausschließlich von Services oder Skripten benutzt werden. Die Nutzung des Kontos darf nicht durch eine Person erfolgen.
- Technische Benutzerkonten dürfen nur mit minimalen Berechtigungen entsprechend dem Berechtigungskonzept konfiguriert werden. Es muss das „Least-Privilege“ Prinzip umgesetzt werden.
- Privilegierte Benutzerkonten dürfen ausschließlich für administrative Tätigkeiten benutzt werden.
- Privilegierte Benutzerkonten für externe Benutzer*innen müssen auf maximal 6 Monate befristet eingerichtet werden und können bei Bedarf nach Ablauf verlängert werden.
- Benutzerkonten für externe Benutzer*innen dürfen nur befristet, jedoch maximal für ein Jahr vergeben werden. Die Befristung muss sich an der Vertragslaufzeit der extern nutzenden Person orientieren. Accounts können ggf. aktiv erneuert werden.

Der Auftragnehmer muss sicherstellen, dass administrative Tätigkeiten nur über personalisierte Konten durchgeführt werden und dass diese Konten ausschließlich für administrative Zwecke genutzt werden.

13 Berechtigungsmanagement

Das ISMS des Auftragnehmers muss ein dokumentiertes Verfahren zur dokumentierten Genehmigung, Vergabe, Änderung, Korrektur, regelmäßigen Aktualisierung und dem zeitnahen Entzug von Berechtigungen enthalten.

Die Berechtigungskonzepte des Auftragnehmers müssen auf den Prinzipien "Need-to-know" und "Least-Privilege " basieren und wirksam durchgesetzt sein.

Im Rahmen des Berechtigungsmanagements müssen die Anforderungen an die Funktionstrennung (Segregation of Duties) umgesetzt werden.

Das Berechtigungskonzept muss technische und organisatorische Maßnahmen beinhalten, welche die Wirksamkeit des Berechtigungskonzepts sicherstellen.

14 Change- und Patchmanagement

Das ISMS des Auftragnehmers muss Verfahren für das Test-, Change- und Patchmanagement in Anlehnung an gängige Standards (z.B. ITIL) beinhalten, dass die sichere, regelmäßige (mindestens alle 6 Monate) und anlassbezogen unverzügliche Implementierung von (Sicherheit-)Patches und Updates für die bereitgestellte Leistung gewährleistet.

15 Trennung von Test- und Produktionsumgebungen

Durch das ISMS des Auftragnehmers und technische Maßnahmen muss sichergestellt sein, dass Schwachstellen, Bedienfehler oder technische Fehler in Testumgebungen kein Risiko für die Produktivumgebung darstellen (z.B. durch Trennung von Testumgebung und Produktionsumgebung durch eine Firewall).

Testumgebungen müssen im Wesentlichen den zugehörigen Produktivumgebungen entsprechen."

16 Management von Sicherheitsvorfällen

Der Prozess zur Erkennung, Priorisierung, Behandlung und Dokumentation von Sicherheitsvorfällen (Security Incidents) und anderen Störungen muss die zentrale Erfassung und Auswertungen von relevanten Loginformationen beinhalten.

17 Schwachstellenmanagement

Der Auftragnehmer muss ein Verfahren zur Erkennung, Bewertung (z.B. CVSS), Priorisierung, Beseitigung und Dokumentation von Schwachstellen für die bereitgestellte Leistung umsetzen.

Der Auftragnehmer muss an die Auftraggeberin quartalsweise über die für die zu erbringende Leistung relevanten erkannten Schwachstellen, sowie deren Bewertung und Beseitigung berichten.

Der Auftraggeber muss ein Verfahren für regelmäßige (mindestens jährlich), automatisierte und protokollierte Schwachstellenscans umsetzen.

18 Härtungskonzept

Der Auftragnehmer muss ein Verfahren zur Härtung der technischen Komponenten umsetzen. Das Verfahren muss insbesondere sicherstellen, dass

- nicht benötigte oder unerwünschte Dienste oder Schnittstellen deaktiviert sind,
- nicht benötigte Benutzerkennungen deaktiviert oder gelöscht sind und
- voreingestellte Passwörter geändert werden.

19 Interne Audits

Der Auftragnehmer muss ein Verfahren umsetzen, das sowohl regelmäßige als auch anlassbezogene Prüfungen der Sicherheitsmaßnahmen auf Angemessenheit und Wirksamkeit (wie zum Beispiel Soll-Ist-Vergleiche von Konfigurationen, Firewall-Regelwerken oder Penetrationstests) beinhaltet und die Prüfergebnisse protokolliert.

Der Auftragnehmer muss nach Ankündigung durch die Auftraggeberin externe Penetrationstests durch sie oder durch Dritte erlauben (maximal jährlich).

Feststellung aus internen Audits und Penetrationstests müssen unverzüglich durch den Auftragnehmer behoben werden. Die Behebung muss durch den Auftragnehmer ohne eine gesonderte Vergütung hierfür erfolgen.

20 Arbeitsplätze von Administratoren

Der Auftragnehmer stellt sicher, dass der Zugang zu Systemen zu Administrationszwecken nur von gehärteten, zugangsbeschränkten und überwachten Arbeitsplätzen erfolgen kann.

21 Schutz vor Schadsoftware

Der Auftragnehmer muss ein Verfahren zum kontinuierlichen Schutz technischer Komponenten vor Schadsoftware und ein Reaktionskonzept für großflächig auftretende Schadsoftware (z.B. Ransomware) umsetzen.

22 Datensicherungskonzept

Der Auftragnehmer muss ein Verfahren für die Datensicherung umsetzen, das regelmäßige und dokumentierte Tests der Wiederherstellung von Datensicherungen beinhaltet.

23 Mandantentrennung

Der Auftragnehmer muss ein technisches Verfahren zur Mandantentrennung umsetzen, das sicherstellt, dass Informationen und Verarbeitungskontexte verschiedener Kunden getrennt gehalten werden.

24 Umgang mit Authentisierungsmitteln

Der Auftragnehmer muss ein Verfahren zur Verwendung, zum sicheren Wechsel, Austausch, Speichern und Hinterlegen von Authentisierungsmitteln (z.B. Passwörtern), sowie eine Regelung zum sicheren Umgang mit Authentisierungsmitteln (z.B. Passwörtern) umsetzen.

Der Missbrauch von Authentisierungsmitteln muss als Sicherheitsvorfall bewertet und behandelt werden.

25 Löschkonzept

Der Auftragnehmer muss ein Verfahren für die Rückgabe, das vollständige Löschen (d.h. nicht rekonstruierbar) und das Vernichten von Daten umsetzen, so dass von der Auftraggeberin als „nicht mehr benötigt“ klassifizierte Daten umgehend gelöscht werden, sofern sie keiner gesetzlichen oder vertraglichen Aufbewahrungs- oder Sperrfrist unterliegen und eine Löschung mit technisch vertretbarem Aufwand möglich ist.

Insbesondere muss dieses Verfahren Anwendung finden für Informationen der Auftraggeberin bei der geplanten oder ungeplanten Beendigung der Leistungserbringung.

Die Löschung ist der Auftraggeberin auf Verlangen und durch entsprechende Erklärung oder anderweitig nachzuweisen. Das Löschverfahren muss auf Anforderung nachgewiesen werden.

26 Sicherer Betrieb von Firewalls

Der Auftragnehmer muss durch ein geeignetes Verfahren sicherstellen, dass alle Firewalls mit einem minimalen Regelwerk (Whitelisting) betrieben werden.

Die Regelwerke müssen dokumentiert sein und der IST-Stand der Regelwerkskonfiguration der Firewalls muss regelmäßig mit dem dokumentierten SOLL-Zustand verglichen werden.

27 Einsatz von Kryptographie – Kryptokonzept

Der Auftragnehmer muss ein Verfahren umsetzen, das den wirksamen Gebrauch von Kryptographie und das Schlüsselmanagement zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen beinhaltet.

Der Auftragnehmer muss bei Übertragung und Speicherung von Daten der Auftraggeberin eine angemessene Verschlüsselung sicherstellen (d.h. sowohl "In Transit" als auch "At Rest").

Insbesondere die Kommunikation über nicht vertrauenswürdige Verbindungen (z.B. WAN, Internet) muss angemessen verschlüsselt erfolgen.

Die Verschlüsselungsprotokolle und -verfahren des Auftragnehmers müssen dem aktuellen Stand der Technik entsprechen.

28 IT-Notfallmanagement

Der Auftragnehmer muss über ein angemessenes, dokumentiertes und implementiertes IT-Notfallmanagement verfügen, welches die zu erbringende Leistung inklusive der verarbeitenden Informationen mit den dazu notwendigen infrastrukturellen, organisatorischen, personellen und technischen Komponenten umfasst.

Das IT-Notfallmanagement des Auftragnehmers muss einem kontinuierlichen Verbesserungsprozess unterliegen.

Das IT-Notfallmanagement muss mindestens die folgenden Szenarien beinhalten:

- Ausfall eines Gebäudes
- Ausfall eines Rechenzentrums
- Ausfall von Kommunikationsinfrastruktur

Notfalltests für diese Szenarien müssen regelmäßig durchgeführt und dokumentiert werden. Die Ergebnisse der Notfalltests müssen zur Verbesserung genutzt werden.