



Anlage E 1: Leistungsbeschreibung

Informationssicherheit Dienstleistung für das Goethe-Institut weltweit

1. Gegenstand der Leistung

1.1 Ausgangssituation

Das Goethe-Institut ist das weltweit tätige Kulturinstitut der Bundesrepublik Deutschland. Mit seinem Netzwerk aus Goethe-Instituten, Goethe-Zentren, Kulturgesellschaften, Lesesälen sowie Prüfungs- und Sprachlernzentren nimmt das Goethe-Institut seit über sechzig Jahren im Auftrag der Bundesrepublik Deutschland weltweit zentrale Aufgaben der auswärtigen Kultur- und Bildungspolitik wahr. Die drei Hauptziele des Instituts sind laut Satzung:

- die Förderung der Kenntnis deutscher Sprache im Ausland
- die Pflege der internationalen kulturellen Zusammenarbeit
- die Vermittlung eines umfassenden Deutschlandbildes durch Informationen über das kulturelle, gesellschaftliche und politische Leben.

Das Goethe-Institut umfasst derzeit neben der in München ansässigen Zentrale rund 150 Institute in ca. 100 Ländern, für die eine komplexe IT-Infrastruktur durch den zentralen IT-Bereich bereitgestellt und betrieben wird.

Wesentliche Komponenten dieser IT-Infrastruktur sind:

- Microsoft Azure hosted und Server-Installationen in den weltweiten Instituten
- SAP-Installationen für Personal, Finanzen und Sprachkursmanagement
- umfangreiches Portfolio an Individual- und Standard-Software sowie Web-Applikationen für Kern Aufgaben für Kultur und Sprachanwendungen
- Microsoft-basierte Arbeitsplatzsysteme und Office- sowie Kommunikationslösung (M365 und Teams)
- komplexe, weltweite Internetplattform
- weltweites Datenkommunikationsnetzwerk (MPLS, DSL)

Zusätzlich wird im Goethe-Institut eine im Rahmen der Digitalisierung wachsende Anzahl an dezentral in Abteilungen und Instituten verantworteten IT-Verfahren eingesetzt. Diese beinhalten sowohl beauftragte Individuallösungen wie auch zunehmend am Markt verfügbare Cloud-Services und KI-Lösungen.



1.2 Zielsetzung / Genereller Leistungsumfang

Aus der beschriebenen komplexen und weltweiten IT-Infrastruktur ergeben sich vielfältige und geschäftskritische Anforderungen hinsichtlich der Informationssicherheit. Allgemeines Ziel der Ausschreibung ist der Abschluss eines EVB-IT-Dienstleistungsvertrags mit einem kompetenten und leistungsfähigen Partnerunternehmen für sämtliche Bereiche der Informationssicherheit.

Generell sind dabei durch den Auftragnehmer folgende Bereiche abzudecken:

1. Generelles Security Consulting	Allgemeines Consulting, Informations- und IT-Sicherheit Strategieberatung (Ausgestaltung eines ISMS), Security Reports, Prozessberatung, Management Feedback, KPI-Festlegung, Definition von Zielwerten in Abstimmung mit AG, sowie Monitoring, Formulierung von IT-Sicherheit Richtlinien (Ausführungsbestimmungen), Policies. Vernetzung und Zusammenarbeit mit ähnlichen Organisationen und Mittler Organisationen im öffentlichen Raum.
2. Information Security Assessments / Tests/Automation	Information Security Assessments und Tests von Fachverfahren (Technik, Prozesse für sämtliche Fach Abteilungen und internationale Regionen (z.B. Personal-, Finanzverfahren, Individualentwicklungen für Kultur und Sprache, ...). Automatisierung der Assessments-Prozesse und BSI-Grundschutz und ähnlicher Vorgaben
3. Sicherheitsarchitektur und Ingenieurtechnik	z.B. Prüfung von technischen Prozessen unter Verwendung sicherer Designprinzipien. Unterstützung in der Gestaltung von grundlegenden Konzepten von Sicherheitsmodellen und Sicherheitsfunktionen von Informationssystemen; Bewertung und Minderung von Schwachstellen in Systemen; Kryptographie, einschließlich Methoden kryptoanalytischer Angriffe und Schlüsselmanagementpraktiken; und Sicherheitsprinzipien, die bei der Gestaltung von Standorten und Einrichtungen angewendet werden. Verwendung von künstlicher Intelligenz zur Automatisierung und Effizienzsteigerung der Informationssicherheit
4. Sicherheits-Operations	z.B.: Cyberermittlungen verstehen und unterstützen; Anforderungen für Untersuchungsarten; (z.B.: Forensik) Auswertung von Logging- und Überwachungsaktivitäten; Sichere Bereitstellung von IT-Ressourcen; (z.B.: Laptops, Desktops, Smart Phones, VR-Brillen, u.a.) Grundlegende Sicherheitsoperationskonzepte;(z.B.: CIS hardened Images); Vorfalls- und Notfallmanagement und Notfallwiederherstellung; Verwaltung der physischen Sicherheit; und Geschäftskontinuität.



5. Identitäts- und Zugriffmanagement (IAM)	z.B. Physischer und logischer Zugriff auf Assets, Identifizierung und Authentifizierung, Integration von Identität als Dienstleistung und Identitätsdiensten von Drittanbietern;(z.B.: ENTRA, Agentische KI) Autorisierungsmechanismen und Lebenszyklus der Identitäts- und Zugriffsbereitstellung.
6. Kommunikations- und Netzwerksicherheit	z.B.: Fortlaufende Unterstützung von sicheren Designprinzipien für die Netzwerkarchitektur; sichere Netzwerkkomponenten; sichere Kommunikationskanäle; und OSI (Open System Interconnection) und TCP/IP (Transmission Control Protocol/Internet Protocol) Modelle.
7. Vertragsprüfungen und -beratung	z.B. Technische und Organisatorische Maßnahmen (TOM)-Prüfung, Teleservicevereinbarung
8. Informations- und IT-Sicherheit-Awareness und Newsletters	Entwicklung spezifischer Informationssicherheits-Trainingsunterlagen für Intranet und für die Schulungsplattform
9. Sicherheits- und Risikomanagement	Unterstützung für die Umsetzung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen (bekannt als CIA-Triade); Grundsätze der Compliance-Verwaltung; und Compliance-Anforderungen; Rechtliche und regulatorische Fragen im Zusammenhang mit der Informationssicherheit; IT-Richtlinien und -Verfahren; risikobasierte Managementkonzepte



2. Leistungsbeschreibung im Einzelnen

1. Generelles Security Consulting.

Strategisches Ziel des Goethe-Instituts ist es Organisation, Prozesse und Infrastruktur im Sicherheitsumfeld entsprechend dem state-of-the-art/ Stand der Technik weiterzuentwickeln.

Dabei sind pragmatische Lösungen zu entwickeln, welche die Arbeit eines weltweit tätigen Kulturinstituts bestmöglich unterstützen, insbesondere auch durch Verwendung von Automatisierung und Künstliche Intelligenz (KI).

Die zu verbessernden und zu implementierenden Prozesse und Policies (ISMS) müssen sich dabei eng an internationale Standards wie ISO 27.000, NIST anlehnen, eine entsprechende Zertifizierung des Goethe-Instituts ist gegenwärtig nicht vorgesehen.

In Analogie zur Rolle des Datenschutzbeauftragten für rechtliche Fragestellungen bietet der externe IT-Sicherheitsbeauftragte Unterstützung für organisatorische und technische Themen. Dies hat in enger Zusammenarbeit mit den verantwortlichen Experten für Informations-Sicherheits-Management des Goethe-Instituts erfolgen.

Vorrangige Aufgaben des Auftragnehmers sind hierbei:

- Monatliche Berichte an die Leitungsebene des Goethe-Instituts über den Stand der Informationssicherheit im Goethe-Institut in Abstimmung mit den internen Experten.
- Aufzeigen von Handlungsoptionen, Prozessoptimierungen und ggf. Organisationsanpassungen
- Erstellung von Berichten zur Informations- und IT-Sicherheit
- Beurteilung und Empfehlung zur Behandlung von Informationssicherheitsrisiken
- Begleitung der Planung und Steuerung zur Behebung von Informationssicherheitsrisiken
- Fortlaufendes Monitoring der Umsetzung und Wirksamkeit von Sicherheitsprozessen, Richtlinien und deren praktischer Umsetzung.
- Unterstützung der Abteilungsleitung und der internen Information Security bei der Wahrnehmung der Aufgaben zur Informationssicherheit
- Beratung zum Monitoring von Informations- und IT-Sicherheitsmaßnahmen im Rahmen des IT-Auditing (Messung, Analyse und Bewertung)
- Erstellen von Informationen zu aktuellen IT-Sicherheitsthemen und Steigerung der Awareness für IT-Sicherheit



Hierbei ist das existierende Informations-Sicherheits-Umfeld einer fortlaufenden Analyse und Bewertung zu unterziehen. Diese Analyse umfasst insbesondere folgende Bereiche:

- Organisation und Prozesse
- Bereitstellungsprozess von Applikationen
- Daten und Informationsprozesse
- Infrastruktur, Betrieb
(Azure, Endgeräte, Netzwerk, Systeme, Software, Applikationen, Cloud-Services, Webapplikationen, M 365/Azure)

Die Analyse zeigt bestehende Schwachstellen auf und liefert im Ergebnis Vorschläge für konkrete Handlungsoptionen. Die Ergebnisse sind sowohl in Form fortlaufender Berichte zur Lage der Informations- und IT-Sicherheit im Goethe-Institut darzustellen als auch in regelmäßigen Feedback-Runden gegenüber der Leitungsebene des Hauses zu erläutern.

Um der aktuellen Informations- und IT-Bedrohungslage im Goethe-Institut bestmöglich Rechnung zu tragen und seine Informations- und IT-Landschaft und diesbezügliche Geschäftsprozesse entsprechend fortlaufend zu verbessern, findet die Analyse vor dem Hintergrund der jeweils aktuellen Entwicklungen im IT-Sicherheitsumfeld statt. Auch sind umfassende Best-practice Erfahrungen öffentlicher wie industrieller Informations- und IT-Anwender integraler Bestandteil der Analysen und Handlungsempfehlungen.

2. Information Security Assessments / Tests

Der Auftragnehmer muss Informations-Sicherheitsanalysen sowohl auf technischer als auch auf fachlicher Ebene durchführen. Er muss auch in der Automatisierung der Assessment Prozesse tätig sein, um ein effektives und pragmatisches ISMS umzusetzen.

In regelmäßig durchzuführenden Informationssicherheit-Assessments sind dabei alle wesentlichen Bereiche (z.B. Personal-/Finanzverfahren, Individuallösungen in Kultur- und Sprachabteilung) des Goethe-Instituts (und seiner weltweiten Niederlassungen) einer umfassenden Prüfung zu unterziehen, die sowohl die eingesetzte Technik wie auch die betreffenden Fachprozesse umfasst. Die Ergebnisse dieser Assessments werden in Abschlussberichten und anschließenden Expertenrunden diskutiert. Wichtiges Ergebnis sind dabei stets auch konkrete und pragmatische Vorschläge zur Lösung von Sicherheitsproblemen und Produkt- wie auch Prozessverbesserungen.



Für neue und teilweise auch bereits eingesetzte IT-Verfahren sind in enger Abstimmung mit dem Datenschutz-Team des Auftraggebers automatisierte IT-Sicherheitskonzepte zu entwickeln. In zunehmendem Maße betrifft dies auch den Einsatz von dem am Markt verfügbarer Cloud-Services. Die zu erstellende Konzepte haben Möglichkeiten zum sicheren Einsatz der entsprechenden Verfahren aufzuzeigen und eine Bewertung ggf. vorliegender Einsatzrisiken sowie Maßnahmen zur Risikominderung zu beinhalten.

In diesem Rahmen sind auch auf Abruf des Auftraggebers ad-hoc Klärungen zu technischen Sicherheitsfragen vom Auftragnehmer zu beantworten, insbesondere bei der Evaluierung neuer Produkte für den Einsatz in Kulturveranstaltungen und im Sprachkursbetrieb.

Die weitmögliche Automatisierung dieser Prozesse ist das primäre Ziel.

3. Sicherheitsarchitektur und Ingenieurtechnik

Im Rahmen der Sicherheitsarchitektur und Ingenieurstechnik ist eine fortlaufende Unterstützung durch den Auftragnehmer bei der Verwendung von sicheren Designprinzipien für die Bewertung technischer Prozesse notwendig, wie ebenfalls die Unterstützung bei der Entwicklung grundlegender Konzepte von Sicherheitsmodellen und Sicherheitsfunktionen innerhalb von Informationssystemen. Die Identifizierung und Behebung von Schwachstellen in Systemen; Kryptographie, einschließlich Methoden kryptoanalytischer Angriffe und Schlüsselverwaltungspraktiken muss der Auftragnehmer erfüllen.

4. Kommunikations- und Netzwerksicherheit

Der Auftragnehmer muss das Goethe-Institut in der State-of-the-art Kommunikations- und Netzwerksicherheit unterstützen. Dies beinhaltet die konsistente Einhaltung sicherer Designprinzipien in der Netzwerkarchitektur, einschließlich sicherer Netzwerkkomponenten, Kommunikationskanäle.

5. Identitäts- und Zugriffsmanagement (IAM)

Der Auftragnehmer muss technische und organisatorische Projekte im Bereich des IAM begleiten. Diese besteht sowohl aus Consulting-Leistungen, wie auch fallweise der temporären Entsendung einzelner Mitarbeiter zur konkreten Projektmitwirkung bzw. Projektleitung bestehen. Mögliche Projekte wären z.B. Implementierung eines organisationsweiten IAM, Einführung einer organisationsübergreifenden IAM Cloud-Governance.



6. Security Operations

Zur Gewährleistung eines sicheren IT-Betriebes ist die Unterstützung des Betriebsteams des Goethe-Instituts und seiner Dienstleister beim Einsatz von Werkzeugen zur pro- und reaktiven Erkennung von Sicherheitsschwachstellen erforderlich. Beispiele hierfür sind: Einsatz von Schwachstellenscanner-Systemen oder eines SIEM etc. Die Unterstützung durch den Auftragnehmer hat hierbei sowohl Beratung wie auch konkrete technische Hilfestellung bei Planung, Einsatz und Auswertung der entsprechenden Tools, Beratung bei Schwachstellenmanagement, Einführung von ein Security Operations Center zu beinhalten.

7. Vertragsprüfungen und -beratung

Der Auftragnehmer muss im Rahmen der Beauftragung von unterschiedlichen Dienstleistern durch das Goethe-Institut eine Beratung und Prüfung der dabei erforderlichen Vertragsunterlagen zur IT- und Informations-Sicherheit durchführen (z.B. Prüfung von technischen und organisatorischen Maßnahmen (TOMs), Teleservicevereinbarungen etc.).

8. IT-Sicherheitsschulungen, Awareness, Newsletters

Ein Bestandteil des Leistungspaketes ist die Erstellung von Unterlagen zur Förderung der Awareness der Gesamtbelegschaft für Fragen der IT- und Informations-Sicherheit. Dies umfasst die Erstellung von Informationsschreiben, Schulungsunterlagen und fallweise auch die Abhaltung von Schulungen zur IT-Sicherheit bei Bedarf des Auftraggebers.

Es ist insbesondere ein Quartals-Newsletter zu aktuellen gemeinsam zu vereinbarenden Sicherheitsthemen zu erstellen.

9. Sicherheits- und Risikomanagement

Der Auftragnehmer muss das Goethe-Institut bei den folgenden Aufgaben unterstützen:

- Risikobewertung: Identifizierung und Bewertung potenzieller Risiken für das Unternehmen, einschließlich physischer Sicherheitsbedrohungen, Cybersicherheitslücken und betrieblichen Risiken.
- Entwicklung und Umsetzung von Richtlinien und Risikoframeworks: Erstellen von Sicherheitsrichtlinien und -protokollen, Sicherstellung der Einhaltung gesetzlicher und behördlicher Anforderungen und regelmäßige Aktualisierung dieser Richtlinien auf der Grundlage neuer Gesetzesvorgaben oder Bedrohungen.
- Berichterstattung: Dokumentation von Vorfällen, Erstellung von Risikobewertungsberichten und Bereitstellung von Empfehlungen an das Management zur Verbesserung von Sicherheitsmaßnahmen.

www.goethe.de



- Kontinuierliche Verbesserung: Beratung über die neuesten Sicherheitstechnologien, Bedrohungslandschaften und Best Practices, um die Sicherheitslage des Auftraggebers kontinuierlich zu verbessern.

10. Implementierungskosten

Die Implementierungskosten sind Kosten, die einmalig zu Vertragsbeginn anfallen, um die nötige Einarbeitung in die Themen der Punkte 1.-9. Im Bezug auf die Herausforderungen des Goethe-Instituts abzudecken, soweit der Bieter nicht der Bestands-Vertragspartner ist. Wir rechnen mit einem Zeitbedarf von ca. 2 Monaten hierfür.

3. Angebots-/Preisstruktur

Für die dargestellten Leistungen ist eine Aufteilung in eine monatlich abzurechnende fixe Pauschalpreis-Komponente sowie per Einzelauftrag nach Aufwand abzurechnende Leistungen gefordert.

In Rahmen der Pauschalpreiskomponenten müssen die Leistungen der Punkte 1., 4. und 8. enthalten sein.

Alle anderen Leistungen werden innerhalb des abzuschließenden Vertrages nach Bedarf per Einzelabruf beauftragt. Hierfür ist durch den Auftragnehmer jeweils ein qualifiziertes Einzelangebot zu erstellen, das die wesentlichen Auftragsinhalte sowie eine Aufwandsschätzung umfasst.