IMF
INGENIEURGESELLSCHAFT
MEINHARDT FULST

Richtlinie

INFORMATIONSSICHERHEIT FÜR LIEFERANTEN UND PARTNER

Ingenieurgesellschaft Meinhardt Fulst GmbH
Kaiserstraße 18
38690 Goslar

Klassifizierung: PUBLIC

Version 1.1
28. Juli 2025

INHALTSVERZEICHNIS

1 Zweck, Anwendungsbereich und Anwender 3
2 Grundsätzliche Regelungen von Vertraulichkeit und dem Schutz personenbezogener Daten 3
3 Regelungen zum Umgang mit Informationen und informationsverarbeitenden Einrichtungen 3
3.1 Allgemeines 3
3.2 Klassifizierung von Informationen 4
3.3 Kennzeichnung von klassifizierten Informationen 5
3.4 Umgang mit klassifizierten Informationen 5
4 Meldung von Sicherheitsschwachstellen und Vorfällen 6
5 Awareness und Überprüfungen 6
6 Kontakt 7
6.1 Informationssicherheitsbeauftragte (ISMS-Ausschuss) 7
6.2 Datenschutzbeauftragter (DSB) 7

1 Zweck, Anwendungsbereich und Anwender

Dieses Dokument gilt verbindlich bei der IMF in allen Standorten, für alle Lieferanten, Dienstleister und Auftragnehmer (weiter: AN) und für alle Arten von Information, unabhängig von deren Form (Papier oder elektronische Dokumente, Anwendungen und Datenbanken, persönliches Wissen, etc.).

In diesem Dokument wird aus Gründen der besseren Verständlichkeit das generische Maskulinum verwendet. Weibliche und weitere Geschlechteridentitäten werden dabei ausdrücklich mitgenannt, soweit es für die Aussage erforderlich ist.

Bei Auslegungsfragen zwischen den verschiedensprachigen Versionen des vorliegenden Vertrages ist die deutsche Fassung maßgebend.

Der Zweck dieses Dokuments ist die Festlegung von Regeln für den Umgang mit Informationen und den Einsatz von Informationstechnik, welche die AN zu befolgen haben.

Die Regeln dienen dem Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der Rechte und Interessen der IMF als Auftraggeberin, sowie aller natürlichen und juristischen Personen, die eine Geschäftsbeziehung mit IMF eingehen und/ oder Tätigkeiten für diese ausführen. Die in diesem Dokument aufgeführten Regeln ergänzen oder konkretisieren die in den, zwischen der IMF und dem Lieferanten und dessen Mitarbeiter vereinbarten, Geheimhaltungsverpflichtungen und/ oder Verträgen zur Auftragsverarbeitung.

2 Grundsätzliche Regelungen von Vertraulichkeit und dem Schutz personenbezogener Daten

IMF arbeitet ausschließlich mit ISMS relevanten Lieferanten und Partnern zusammen, welche sich zur Wahrung von Vertraulichkeit von Daten, Informationen und Geschäftsgeheimnissen im Rahmen der entsprechenden Verpflichtungserklärung oder einer anderweitigen Geheimhaltungsvereinbarung (kurz NDA) verpflichtet haben.

Erfolgt durch den AN eine Verarbeitung personenbezogener Daten im Auftrag der IMF, so ist vor Aufnahme der beauftragten Tätigkeit zusätzlich ein Auftragsverarbeitungsvertrag (kurz AVV) abzuschließen.

Daten und Informationen über IMF bzw. solche, die aus der Aufgabenerfüllung bekannt werden, dürfen nicht an Dritte weitergegeben bzw. veröffentlicht werden, insbesondere nicht in sozialen Netzwerken (z. B. Facebook, google+, LinkedIn, XING ...) oder anderweitig, insbesondere im Internet (z. B. Twitter, Youtube …). Ausnahmen liegen nur dann vor, wenn es sich um allgemein zugängliche Daten handelt, das Vertragsverhältnis spezifisch eine solche Weitergabe bzw. Veröffentlichung von Daten vorsieht oder eine ausdrückliche Zustimmung der IMF vorliegt.

3 Regelungen zum Umgang mit Informationen und informationsverarbeitenden Einrichtungen

3.1 Allgemeines

Sollte es im Zusammenhang mit der vertraglichen Aufgabenerfüllung notwendig sein, dass der AN Daten oder Informationen außerhalb der Systeme der IMF verarbeiten bzw. speichern muss, so ist die IMF vor Beginn der Verarbeitung bzw. Speicherung von dem Lieferanten darüber schriftlich zu informieren. Die IMF muss hierzu ihre Zustimmung geben, es sei denn, dass sich dies bereits unmissverständlich aus dem Vertrag ergibt.

Das Entfernen bzw. die Mitnahme seitens der IMF zur Aufgabenerfüllung zur Verfügung gestellter Hard- und Software aus den Standorten der IMF ist ohne ausdrückliche Erlaubnis von IMF untersagt. Eigenmächtige Erweiterungen der von der IMF zur Verfügung gestellten Hardware und das Anschließen von Peripheriegeräten und externen Speichergeräten ist ebenfalls ohne die ausdrückliche Erlaubnis der IMF untersagt. Umbauten bzw. Erweiterungen sind ausschließlich durch die Systemverantwortlichen der IMF durchzuführen.

Sollte der AN für die Erfüllung seiner vertraglichen Aufgaben das E-Mail-System, das Netzwerk bzw. die IT-Systeme der IMF nutzen wollen, so ist er verpflichtet, sich vor Nutzung der Dienste oder Anschluss jeglicher Systeme die ausdrückliche Erlaubnis einzuholen. Weiterhin hat sich der AN regelmäßig bei dem jeweils benannten Ansprechpartner der IMF über die aktuellen internen Regeln zum Umgang mit diesen Systemen und Medien zu informieren und diese Regeln einzuhalten. So ist z. B. die Weitergabe von Konfigurations- und Zugangsdaten, wie auch von Identifikationsmitteln, ohne schriftliche Genehmigung der IMF unzulässig und stellt einen meldepflichtigen Vorfall dar. IMF behält sich vor, auf alle zur Verfügung gestellten Systeme sowie Daten und Informationen ohne Vorankündigung zuzugreifen.

Eine Nutzung der Systeme und Medien der IMF zu privaten Zwecken ist ausdrücklich verboten. Die Nutzung von privaten Geräten der Mitarbeiter oder Erfüllungsgehilfen des AN zur Erfüllung der mit der IMF vertraglich vereinbarten Leistung ist ebenso ausdrücklich verboten, auch wenn dies beim AN intern durch entsprechende Richtlinien geregelt und zulässig ist.

Bei der Verarbeitung von Informationen der IMF durch den AN, sind die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität gemäß dem aktuellen Stand der Technik sicherzustellen. Entsprechend wirksame Maßnahmen des AN, wie z. B. der Schutz vor Schadcode, Zugangs-, Zutritts- und Zugriffskontrollen, Clear-Desk und Clear-Screen, Backup von Informationen, Sensibilisierung und Schutz der Mitarbeiter usw., werden vorausgesetzt.

3.2 Klassifizierung von Informationen

Die IMF klassifiziert Informationen gemäß des Schutzbedarfs bei der Vertraulichkeit unter Berücksichtigung der weiteren Schutzziele Integrität und Verfügbarkeit. Hierbei kommen vier unterschiedliche Informationsklassifizierungen zum Einsatz:

- PUBLIC – die Informationen sind öffentlich
- INTERNAL – die Informationen sind für alle Mitarbeiter und durch IMF ausgesuchte Dritte bzw. AN verfügbar
- CONFIDENTIAL – Die Informationen sind nur einer spezifischen Gruppe von Mitarbeitern und durch IMF autorisierten Dritten zugänglich
- TOP SECRET – die Informationen sind nur einzelnen Mitarbeitern zugänglich, sofern diese Information mit externen begründet ausgetauscht werden, muss die persönliche Zustellung sichergestellt werden

3.3 Kennzeichnung von klassifizierten Informationen

Um über den Schutzbedarf von Informationen vor Kenntnisnahme zu informieren, sollten als „CONFIDENTIAL“ und „TOP SECRET“ klassifizierte Informationen soweit möglich gekennzeichnet werden. Dies kann z.B. durch Beschriftung von Aktenordnern, Projektmappen, Hinweisen in E-Mail-Betreffzeilen, im Dateinamen, in Kopf- oder Fußzeilen von Dokumenten, in Briefen z. B. durch einen inneren Umschlag mit der Ergänzung „vertraulich - zu Händen …“ etc. geschehen.

Der AN ist dafür verantwortlich, seine Mitarbeiter und Erfüllungsgehilfen entsprechend zu informieren und entsprechende Maßnahmen zum Schutz der Informationen einzuleiten.

3.4 Umgang mit klassifizierten Informationen

Insbesondere die Verarbeitung von Informationen die im Rahmen der Zusammenarbeit als „CONFIDENTIAL“ oder „TOP SECRET“ klassifiziert und gekennzeichnet wurden, unterliegen einem besonderen Schutzbedarf. Der AN, dessen Mitarbeiter und dessen Erfüllungsgehilfen dürfen Informationen entsprechend der Klassifizierung nur im genehmigten oder beauftragten Rahmen, nach dem „Need-to-know-Prinzip“ weitergeben. Darüber hinaus sind folgende Maßnahmen zum Schutz der Informationen technisch umzusetzen:

- Bei der Speicherung entsprechend gekennzeichneten Informationen ist vom AN eine strikte Zugriffskontrolle sowie eine angemessene Mandantentrennung zu gewährleisten.
- Eine Verarbeitung, insbesondere Speicherung von als „CONFIDENTIAL“ oder „TOP SECRET“ klassifizierter Informationen im EU-Ausland, zum Beispiel im Rahmen der Nutzung eines Cloud-Dienstleisters, ist nur nach ausdrücklicher Erlaubnis von der IMF gestattet.
- Sofern für die notwendige Speicherung und Verarbeitung seitens des AN Clouddienste genutzt werden, die nicht ausschließlich unter dessen eigener Kontrolle stehen, so sind die als „CONFIDENTIAL“ oder „TOP SECRET“ klassifizierten Informationen der IMF zusätzlich durch Verschlüsselung und einer Multifaktor-Authentifizierung (MFA) vor unbefugtem Zugriff zu schützen. Eventuell in Clouddienste ausgelagerte Backups müssen vor der Übertragung verschlüsselt werden.
- Als „CONFIDENTIAL“ oder „TOP SECRET“ klassifizierte Informationen dürfen nicht unverschlüsselt auf mobilen Datenträgern und Endgeräten gespeichert werden (Notebook, Smartphone, USB-Datenträger etc.).
- Bei dem Transport oder Übertragung durch öffentliche Netzwerke von als „CONFIDENTIAL“ oder „TOP SECRET“ klassifizierter Informationen, sind diese grundsätzlich angemessen nach dem Stand der Technik zu verschlüsseln. Dies betrifft insbesondere auch die Kommunikation per E-Mail.
- Nach Beendigung oder ggf. Änderung des Vertragsverhältnisses sowie nach Ablauf von regulatorischen Fristen müssen die betreffenden Informationen an IMF zurückgegeben bzw. nach Weisung der IMF gelöscht werden. Für den Fall einer gesetzlich auferlegten Archivierungs- bzw. Aufbewahrungspflicht des AN, die über die Dauer der vertraglichen Zusammenarbeit hinausgeht, ist das Schutzniveau der klassifizierten Informationen bis zur Löschung oder Vernichtung aufrecht zu halten.
- Bei der Vernichtung oder Löschung von Daten/Informationen und Informationsträgern (hierzu gehören neben elektronischen Datenträgern auch Papierakten), sind diese gemäß Sicherheitsstufe 3 für als „CONFIDENTIAL“ und Sicherheitsstufe 4 für als „TOP SECRET“ klassifizierter Informationen, nach DIN 66399 zu entsorgen.

4 Meldung von Sicherheitsschwachstellen und Vorfällen

Definition: Sicherheitsschwachstelle - es ist noch kein Vorfall aufgetreten, jedoch könnte das mit einem System, Prozess oder einer Organisation in Zusammenhang stehende Ereignis in naher oder ferner Zukunft einen Vorfall zur Folge haben. Ein Risiko hat sich noch nicht materialisiert, das bedeutet, eine Bedrohung hat die Schwachstelle noch nicht ausgenutzt.

Beispiele für Sicherheitsschwachstellen sind:

- wiederkehrend nicht umgesetzte, technische und organisatorische Maßnahmen

Definition: Vorfall - ein Vorfall, der Schaden durch den Verlust der Vertraulichkeit oder Integrität und damit einhergehend Authentizität von Informationen verursachen kann oder der eine Unterbrechung der Verfügbarkeit von Informationen und/oder Prozessen verursachen könnte. Beispiele für Vorfälle sind:

- Hackerangriffe
- Schadcode- oder Ransomwarebefall
- Abfluss von vertraulichen Informationen oder Authentifizierungsdaten sowie Datenschutzpannen
- Verlust von Arbeitsmitteln, wie z. B. IT-Geräte, mit denen Daten der IMF verarbeitet bzw. gespeichert werden oder auch als Identifikationsmittel bereitgestellt wurden (z.B. Schlüssel, Ausweise oder kryptographische Token)
- Unterbrechung der Verfügbarkeit von IT-Systemen oder Clouddiensten mit Auswirkungen auf die Wertschöpfungskette

Der AN, dessen Mitarbeiter und Erfüllungsgehilfen müssen jegliche Vorfälle, bei dem bei der IMF benannten Vertragsverantwortlichen und der Geschäftsführung melden, sofern die Informationen oder personenbezogenen Daten der IMF betroffen seien, können.

Darüber hinaus muss der AN, dessen Mitarbeiter und Erfüllungsgehilfen erkannte Sicherheitsschwachstellen, an Systemen oder Prozessen die dem Schutz als „CONFIDENTIAL“ oder „TOP SECRET“ klassifizierte Informationen der IMF dienen, bei dem bei IMF benannten Vertragsverantwortlichen und der Geschäftsführung melden.

Die Meldung von Vorfällen und Sicherheitsschwachstellen muss in Textform erfolgen (z.B. E-Mail), ist als solche mindestens als „CONFIDENTIAL“ zu klassifizieren und muss folgende Informationen beinhalten:

- Art (Kurzbeschreibung) des Vorfalls bzw. der Schwachstelle
- Betroffene Art der Informationen (Klassifizierung, Personenbezug, Anzahl/Umfang der Datenmengen)
- Zeitpunkt des Eintritts und oder der ersten Kenntnisnahme
- Durchgeführte Erstmaßnahmen und oder geplante Maßnahmen zur Behandlung
- Verantwortlicher Ansprechpartner und dessen Kontaktinformationen

5 Awareness und Überprüfungen

Der AN muss die in diesem Dokument enthaltenen Regelungen zur Informationssicherheit in seinem Verantwortungsbereich sicherstellen. In diesem Kontext hat der AN sicherzustellen, dass alle betreffenden Mitarbeiter und Erfüllungsgehilfen ausreichend sensibilisiert, mit den Regelungen vertraut gemacht werden und diese einhalten.

Die IMF hat das Recht, in Abstimmung mit dem AN Überprüfungen der Einhaltung dieser Sicherheitsrichtlinien im erforderlichen Umfang durchzuführen oder durch die im Einzelfall zu benennendem Prüfer durchführen zu lassen. Der IMF sind durch den AN alle Auskünfte zu erteilen, die zur Erfüllung der Kontrollfunktion benötigt werden. Der AN hat bei Vertragsänderung oder Vertragsende der IMF auf Aufforderung mitzuteilen, welche vertraulichen Informationen zurückgesendet oder vernichtet und welche aufbewahrt wurden. Die Mitteilung, dass bestimmte Unterlagen oder Informationen aufbewahrt wurden, ist zu begründen.

Der AN ist im Rahmen der Zusammenarbeit aufgefordert, sich regelmäßig und selbstständig über die aktuellen Regelungen und Richtlinien bei der IMF zu informieren und diese einzuhalten.

6 Kontakt

6.1 Informationssicherheitsbeauftragte (ISMS-Ausschuss)

Zur Meldung von Informationssicherheitsvorfällen und Schwachstellen wenden Sie sich bitte an unseren ISMS-Ausschuss, Tel +49 (0) 5324/7799-0 , E-Mail: ISMS_Ausschuss@i-mf.de

6.2 Datenschutzbeauftragter (DSB)

Bei Fragen zum Datenschutz steht Ihnen unser Datenschutzbeauftragter, das Team der Kämmer Consulting, gerne zur Verfügung. Tel +49 (0) 531/702249-0, E-Mail: dsb-team@kaemmer-consulting.de