Informationssicherheitsstandard für Fremdfirmen

Inhaltsverzeichnis

1 Zweck

Informationen gehören zu den wichtigsten Vermögenswerten der Unternehmensgruppe Eberspächer („Eberspächer Gruppe“). Aufgrund der strategischen Bedeutung, die Informationen für die Eberspäche Gruppe haben, stellen die Verfügbarkeit, Vertraulichkeit und Integrität aller Informationen Schlüsselfaktoren bei der Zusammenarbeit mit Fremdfirmen dar.

Um die Erfüllung dieser Werte und die Beachtung von Rechten und Interessen der Eberspächer Gruppe sowie aller natürlicher und juristischer Personen, die in einer geschäftlichen Beziehung mit der Eberspächer Gruppe stehen sicherzustellen, sind Vorgaben im Hinblick auf die Sicherheit von Informationen notwendig.

Dieser Standard beschreibt konkrete Regelungen und Anforderungen zum sicheren Umgang mit Informationswerten der Eberspächer Gruppe (im Folgenden auch: „Eberspächer“ oder „Auftraggeber“) und richtet sich an die Geschäftsführung von Fremdfirmen, deren Mitarbeiter sowie weitere bei der Aufgabenerfüllung Beteiligte (im Folgenden: „Auftragnehmer“).

2 Geltungsbereich

Dieses Dokument ist für alle Auftragnehmer der Eberspächer Gruppe verbindlich.

EBOS-Submodul: Business Management

3 Definitionen/Benennungen/Abkürzungen

Fremdfirmen	Zu den Fremdfirmen zählen Lieferanten und Dienstleister, die im Auftrag einer Gesellschaft der Eberspächer Gruppe Leistungen erbringen.
GHV	Geheimhaltungsvereinbarung
Informations-verantwortliche/r	Informationsverantwortliche sind zuständig für die Klassifizierung einer Information, bestimmen den erlaubten Empfängerkreis und autorisieren Zugriffe (z. B. durch Vergabe/Genehmigung von Berechtigungen).

4 Vorgaben für Fremdfirmen

I	HINWEIS
In diesem Dokument referenzierte Standards der Eberspächer Gruppe können auf Anfrage der Fremdfirma durch den internen Ansprechpartner bei Eberspächer bereitgestellt werden, sofern diese nicht über das Eberspächer-Lieferantenportal einsehbar sind.	

4.1 Klassifizierung und Kennzeichnung von Informationswerten

Die in diesem Standard beschriebenen Vorgaben sind für sämtliche Informationswerte der Eberspächer Gruppe anzuwenden. Neben Informationen, die auf elektronischen Datenträgern gespeichert sind, zählen hierzu insbesondere auch Papierdokumente, Gespräche sowie Prototypen. Diesbezüglich relevante Informationen sind durch den Auftragnehmer selbstständig zu identifizieren und entsprechend ihrer Klassifikation zu behandeln.

Die Klassifikation von Informationen erfolgt anhand der Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität. Ein entsprechendes Klassifikationsschema und Praxisbeispiele sind im *Informationssicherheitsstandard – Klassifizierung von Informationen und Systemen* beschrieben.

Vertrauliche („Confidential“) sowie Streng Vertrauliche („Strictly Confidential“) Informationen müssen als solche explizit gekennzeichnet und mit besonderer Vorsicht behandelt werden.

4.2 Datenschutz

Die Erhebung und Verarbeitung von personenbezogenen Daten ist nur zulässig, wenn dies mit Eberspächer vereinbart ist und entsprechende vertragliche Regelungen (z.B. Auftragsverarbeitungsvertrag) abgeschlossen wurden, welche nähere Bestimmungen z. B. zu technischen und organisatorischen Schutzmaßnahmen treffen.

4.3 Sicherstellung der Vertraulichkeit und Integrität

4.3.1 Allgemeine Regelungen

Geschäftliche Informationen müssen vor unbefugter Einsichtnahme, Manipulation und Löschung geschützt werden. Grundsätzlich ist das **„Need-To-Know“-Prinzip** anzuwenden, sodass nur diejenigen Personen Zugriff auf Informationen haben, welche diesen für die Erledigung ihrer vereinbarten Aufgaben benötigen. Der Zugriff darf ausschließlich zweckgebunden im Rahmen der Aufgabenerfüllung erfolgen.

Die Weitergabe von Informationen der Eberspächer Gruppe mit **hohem Schutzbedarf** (Vertraulichkeit: *Vertraulich*) oder **sehr hohem Schutzbedarf** (Vertraulichkeit: *Streng Vertraulich*) an Dritte ist ohne Zustimmung des Informationsverantwortlichen untersagt. Voraussetzung für die Weitergabe ist eine gültige Geheimhaltungsvereinbarung (GHV) mit der dritten Partei.

4.3.2 Zugriffsschutz

Die Zugriffsmöglichkeiten auf Informationen der Eberspächer Gruppe sind durch geeignete technische Maßnahmen einzuschränken. Der Zugriff darf nur befugten Personen im Rahmen der Aufgabenerfüllung gewährt werden (z. B. durch Vergabe von Systemberechtigungen). Autorisierte Personen müssen auf die Geheimhaltung verpflichtet sein.

Für den Zugriff auf Informationen sind grundsätzlich personalisierte Benutzerkonten zu verwenden – Ausnahmen müssen durch die IT-Organisation von Eberspächer freigegeben werden.

Die Weitergabe von Anmeldeinformationen (z. B. Benutzername und Passwort) ist verboten. Passwörter sind nach den Vorgaben des *Informationssicherheitsstandard – Passwörter* zu wählen und zu schützen.

Fernzugriffe auf die interne IT-Infrastruktur der Eberspächer Gruppe dürfen nur nach Absprache und Genehmigung erfolgen. Die Vorgaben des *Informationssicherheitsstandards – Fernzugriff* sind hierbei einzuhalten.

Der Zugriff auf informationsverarbeitende Systeme innerhalb der IT-Infrastruktur der Eberspächer Gruppe kann aus Gründen der Nachvollziehbarkeit protokolliert werden.

4.3.3 Zugangsschutz

Der Zugang zu nicht-öffentlichen Informationen der Eberspächer Gruppe ist durch geeignete physische Maßnahmen einzuschränken. Der Zugang darf nur befugten Personen im Rahmen der Aufgabenerfüllung gewährt werden (z. B. durch Vergabe von Zutrittsberechtigungen). Autorisierte Personen müssen auf die Geheimhaltung verpflichtet sein.

Der Zugang zu Schutzzonen auf Betriebsgeländen der Eberspächer Gruppe kann aus Gründen der Nachvollziehbarkeit protokolliert werden.

4.4 Sicherstellung der Verfügbarkeit

Die Verfügbarkeit geschäftlicher Informationen muss seitens des Auftragnehmers durch geeignete technische und organisatorische Maßnahmen sichergestellt werden (z. B. regelmäßige Backups). Der dauerhafte Verlust von Informationen oder Geräten der Eberspächer Gruppe ist unverzüglich anzuzeigen.

Der Auftragnehmer muss darüber hinaus ausreichend personelle und sachliche Ressourcen zur Verfügung stellen, um die Erbringung der vereinbarten Leistungen auch im Störungsfall gewährleisten zu können. Vertragliche Regelungen zum geforderten Servicegrad sind hierbei zu beachten.

4.5 Austausch von Informationen

Beim Austausch von nicht-öffentlichen Informationen ist zu beachten:

- Der Kommunikationspartner muss über die Klassifikation der Informationen (Kriterium: Vertraulichkeit) informiert werden, sofern diese nicht bereits gekennzeichnet sind.
- Informationen sind entsprechend Ihrer Klassifikation zu kennzeichnen.
- Das unbefugte Ab-/Mithören der Kommunikation ist zu unterbinden. Informationen, die über öffentliche Netze versendet werden, sind entsprechend dem *Informationssi-*

cherheitsstandard – Sichere Kommunikation zu schützen. Die Kommunikation per Telefon ist von technischen Schutzmaßnahmen ausgenommen und aus diesem Grund auf den unbedingt erforderlichen Inhalt zu beschränken.

4.6 Schutz von Soft- und Hardware

4.6.1 Bereitstellung

Im Rahmen der Aufgabenerfüllung benötigte Soft- und Hardware kann gegebenenfalls und nach Rücksprache durch die Eberspächer Gruppe bereitgestellt werden. Grundsätzlich ist die Speicherung und Verarbeitung von geschäftlichen Informationen nur auf solchen Endgeräten erlaubt. Insbesondere die Nutzung nicht freigegebener Cloud-Services ist in diesem Zusammenhang untersagt. Ausnahmen von diesen Regelungen müssen durch den internen Ansprechpartner bei Eberspächer in Abstimmung mit der IT-Organisation der Eberspächer Gruppe freigegeben werden.

Informationen, die nicht im Zusammenhang mit der Aufgabenerfüllung stehen (z. B. private Informationen, Informationen von anderen Kunden) dürfen nicht auf Geräten der Eberspächer Gruppe gespeichert oder verarbeitet werden.

Der Auftragnehmer ist für die ordnungsgemäße Nutzung der ihm zur Verfügung gestellten Soft- und Hardware im Rahmen seiner Aufgaben verantwortlich. Die Eberspächer Gruppe behält sich das Recht vor, die Bereitstellung jederzeit zu beenden.

4.6.2 Installation und Veränderung

Die Installation von Soft- und Hardware auf Geräten bzw. im Netzwerk der Eberspächer Gruppe darf nur nach Rücksprache mit dem internen Ansprechpartner sowie der IT-Organisation der Eberspächer Gruppe erfolgen. Fremdgeräte (z. B. Laptops, Smartphones) dürfen nur nach Absprache mit dem Unternehmensnetzwerk verbunden werden.

*	**TIPP**
Fremdgeräte können an Eberspächer-Standorten über ein Gast-Netzwerk auf das Internet zugreifen. Der Zugang muss durch den internen Ansprechpartner vorab beantragt werden.	

Die selbstständige Veränderung der zur Verfügung gestellten Soft- und Hardware ist nicht gestattet (z. B. Konfiguration des Betriebssystems). Manuelle Änderungen dürfen nur in Abstimmung mit der IT-Organisation der Eberspächer Gruppe vorgenommen werden.

Durch Eberspächer bereitgestellte Software- oder Betriebssystem-Updates müssen unverzüglich installiert werden.

4.6.3 Schutz von Datenträgern

Elektronische Daten sind nach Möglichkeit auf den zur Verfügung gestellten Austauschplattformen (z. B. Intranet, Sharepoint, FileExchange) und nicht auf lokalen Datenträgern (z. B. Laptop-Festplatte oder mobile Datenträger) zu speichern, da nur dort eine regelmäßige und automatische Datensicherung gewährleistet ist. Für die Sicherung der Daten, die nicht auf zentralen Systemen gespeichert werden ist der Auftragnehmer selbst verantwortlich.

Beim Einsatz von mobilen Datenträgern ist darauf zu achten, dass immer nur die nötigsten Informationen gespeichert und nicht mehr benötigte Informationen gelöscht werden.

Nicht-öffentliche Informationen dürfen grundsätzlich nur auf verschlüsselten Datenträgern gespeichert werden. Ausnahmen sind von der IT-Organisation freizugeben.

4.6.4 Rückgabe und Löschung

Nicht mehr benötigte Geräte und Datenträger sind unverzüglich, spätestens aber bei Vertragsende, beim Auftraggeber zurückzugeben. Auf Datenträgern des Auftragnehmers gespeicherte Informationen müssen bei Vertragsende vollständig an Eberspächer übergeben und anschließend sicher gelöscht werden. Vertraglich definierte Aufbewahrungs- und Löschfristen sind hierbei einzuhalten.

4.7 Physische Sicherheit

Alle zur Verfügung gestellten Informationswerte (z. B. Dokumente, Prototypen) und Geräte sind sachgemäß zu behandeln und vor Verlust und Diebstahl zu schützen.

Überlassene Geräte und Informationen dürfen das Firmengelände der Eberspächer Gruppe nur mit Genehmigung des Auftraggebers verlassen.

Beim Verlassen des Arbeitsplatzes sind Geräte im laufenden Betrieb vor unbefugtem Zugriff zu schützen (z. B. passwortgeschützte Bildschirmsperre).

Es ist sicherzustellen, dass Geräte mit nicht-öffentlichen Informationen so aufgestellt werden, dass die Einsichtnahme unbefugten Dritten nicht möglich ist. Dies gilt sowohl innerhalb als auch außerhalb des Firmengeländes der Eberspächer Gruppe.

Der Verlust von Informationswerten und Geräten der Eberspächer Gruppe ist unverzüglich zu melden. Dies gilt auch, falls diese nach kurzer Zeit wieder auffindbar sind aber nicht sichergestellt werden kann, dass in diesem Zeitraum kein Unbefugter Zugriff darauf hatte.

I	**HINWEIS**
Standortspezifische Regelungen zur physischen Sicherheit (z. B. besondere Schutzzonen, Fotografierverbot) können über den internen Ansprechpartner bei Eberspächer bereitgestellt werden.	

4.8 Sichere Softwareentwicklung

Wird im Rahmen der Aufgabenerfüllung Software-Code verändert oder erzeugt, so sind Regelungen zur sicheren Softwareentwicklung (Secure Coding Guidelines) für den spezifischen Anwendungsfall mit dem Auftraggeber abzustimmen und einzuhalten. Die IT-Organisation der Eberspächer Gruppe ist über die Entwicklung und Lieferung von Software in Kenntnis zu setzen.

4.9 Meldepflichten

Der Auftragnehmer ist dazu verpflichtet, die Eberspächer Gruppe unverzüglich über Ereignisse und Risiken mit Relevanz für die Informationssicherheit zu informieren.

Hierzu gehören:

- **Verletzung von Gesetzen, vertraglichen Regelungen und Vorgaben**
- **Informationssicherheitsvorfälle** (z. B. Verdacht auf Schadsoftwarebefall)
- **Datenschutzvorfälle** (z. B. Offenlegung personenbezogener Daten)
- **Identifizierte Risiken** (z. B. Schwachstellen in IT-Systemen)

*	**TIPP**
Für Fremdfirmen relevante Kontaktadressen für die Meldung von Ereignissen und Vorfällen in den Bereichen Informationssicherheit und Datenschutz sind im Kapitel 4.12 dieses Dokumentes zu finden.	

Der Auftragnehmer muss meldepflichtige Vorfälle in seinem Verantwortungsbereich dokumentieren, analysieren und durch geeignete Maßnahmen beheben.

Jegliche Änderungen seitens des Auftragnehmers, die Auswirkungen auf die Informationssicherheit der Eberspächer Gruppe haben, müssen vorab einer Prüfung unterzogen und zeitnah gemeldet werden (z. B. Standortwechsel, Änderungen an der IT-Infrastruktur).

Der Auftragnehmer ist darüber hinaus verpflichtet, nicht länger benötigte Berechtigungen (z. B. für IT-Systeme oder Zugangskontrollen) unverzüglich anzuzeigen.

I	**HINWEIS**
Weiterführende Vorgaben und Regelungen zur Meldung von Informationssicherheitsvorfällen sind im *Informationssicherheitsstandard – Sicherheitsvorfallmanagement* beschrieben.	

4.10 Einhaltung der Vorgaben

Die Einhaltung der in diesem Standard definierten Anforderungen an die Informationssicherheit muss seitens des Auftragnehmers gewährleistet werden. Innerhalb der Organisation des Auftragnehmers sind zu diesem Zweck klare Verantwortlichkeiten für die Einhaltung und Umsetzung der beschriebenen Vorgaben zuzuweisen. Insbesondere sind Angestellte des Auftragnehmers auf die Einhaltung der Informationssicherheitsvorgaben zu verpflichten.

Neben den spezifischen Richtlinien der Eberspächer Gruppe sind die im Land des Auftraggebers gültigen gesetzlichen Regelungen zum Daten- und Informationsschutz einzuhalten. Bei Auslandsreisen sind die länderspezifischen Vorgaben zur Informationssicherheit zu beachten.

Geistige Eigentumsrechte sind zu wahren. Hierzu zählen z. B. Urheberrechte, Bildrechte, Rechte an Entwürfen oder Quellcodelizenzen. Überlassene Softwarelizenzen dürfen nur für den vereinbarten Zweck und in Übereinstimmung mit der Lizenzvereinbarung des Herstellers verwendet werden. Der Einsatz von nicht-lizenzierter Software ist gemäß gesetzlichen Bestimmungen verboten.

Sämtliche Informationssicherheitsvorgaben der Eberspächer Gruppe sind auch für Unterauftragnehmer verbindlich. Der Auftragnehmer ist dafür verantwortlich, die Einhaltung der Vorgaben bei Unterauftragnehmern sicherzustellen.

Eine Abweichung von den Informations- und IT-Sicherheitsstandards ist nur in Abstimmung mit dem Informationssicherheitsbeauftragten der Eberspächer Gruppe (zeitlich begrenzt) zulässig.

Die Nichteinhaltung oder Verletzung der gültigen Regelungen werden individuell nach betrieblichen und rechtlichen Vorschriften geprüft und entsprechend geahndet.

4.11 Überprüfung

Die Erkennung und Vermeidung von Schwachstellen und Sicherheitslücken setzt eine regelmäßige Überprüfung der Informationssicherheit voraus. Insbesondere ist in diesem Zuge die Einhaltung der gesetzlichen und vertraglich definierten Anforderungen und Vorgaben zu prüfen.

Der Auftragnehmer ist dazu verpflichtet, die Einhaltung der relevanten Anforderungen und Vorgaben zur Informationssicherheit in seiner Organisation regelmäßig zu überprüfen. Weiterhin sind eventuelle Unterauftragnehmer ebenfalls einer regelmäßigen Prüfung zu unterziehen.

Die Eberspächer Gruppe behält sich darüber hinaus vor, die Einhaltung der relevanten Anforderungen und Vorgaben zur Informationssicherheit beim Auftragnehmer zu prüfen. Der Auftragnehmer ist dazu verpflichtet, die Überprüfung durch Bereitstellung von Selbstbeurteilungen („Self Assessment“) sowie geeigneten Nachweisen zu unterstützen.

4.12 Kontakt

Für fachspezifische Fragen sowie zur Meldung von sicherheitsrelevanten Ereignissen, Vorfällen und Änderungen stehen folgende Kontaktmöglichkeiten zur Verfügung:

Ansprechpartner Informationssicherheit: global-itsec@eberspaecher.com

Ansprechpartner Datenschutz: datenschutz@eberspaecher.com

5 Mitgeltende Dokumente

Dokumentart	Nomenklatur, Titel und Hyperlink
Formblatt	EB-F-3671 Geheimhaltungsvereinbarung
Standard	EB-S-9102 Klassifizierung von Informationen und Systemen
Standard	EB-S-5033 Passwörter
Standard	EB-S-4911 Fernzugriff
Standard	Sichere Kommunikation
Standard	EB-S-9076 Sicherheitsvorfallmanagement
Standard	DEU-I-697 Richtlinien für Fremdfirmen
Standard	ET-S-9052 Information security aspects in supplier relationship
Flyer	EB-I-5817 Informationssicherheit - Fremdfirmen