

## **Informationssicherheitsanforderungen der Flughafen Hannover-Langenhagen GmbH**

### **Inhalt**

1. Änderungshistorie .....	3
2. Einleitung und Geltungsbereich.....	3
3. Allgemeine Sicherheitsanforderungen .....	3
3.1. Umgang mit Informationen des Auftraggebers.....	3
3.1.1. Zugriffssteuerung .....	3
3.1.2. Übertragungswege .....	3
3.1.3. Ablage und Aufbewahrung .....	4
3.1.4. Vernichtung und Entsorgung .....	4
3.2. Meldung von Informationssicherheitsvorfällen .....	4
3.2.1. Definition Informationssicherheitsvorfälle .....	4
3.2.2. Meldepflicht und Meldefristen .....	4
3.2.3. Zu meldende Informationen .....	5
3.3. Sensibilisierung und Verpflichtung der Mitarbeiter.....	5
3.4. Durchführung von Dienstleister-Audits .....	5
3.5. Regelungen zum Ende der Tätigkeiten .....	5
3.6. Weitergabe der Sicherheitsanforderungen an Unterauftragnehmer .....	6
4. Sicherheitsanforderungen für Arbeiten mit Systemen des Auftraggebers .....	6
4.1. Arbeiten an IT-Systemen .....	6
4.2. Umgang mit Clients des Auftraggebers.....	6
4.3. Umgang mit Zugangsdaten .....	6
5. Besondere Sicherheitsanforderungen für Arbeiten an IT-Systemen innerhalb der Räumlichkeiten des Auftraggebers .....	7
5.1. Zugang zu Remote-Systemen.....	7
5.2. Umgang mit Remote-Zugangsdaten .....	7
5.3. Protokollierung der Tätigkeiten .....	7
6. Sicherheitsanforderungen für Arbeiten an Systemen in Räumlichkeiten des Auftragnehmers.....	7
6.1. Sichere Aufbewahrung.....	7
6.2. Sicherer Transport .....	7
6.3. Protokollierung der Tätigkeiten .....	8
7. Sicherheitsanforderungen für die Verarbeitung von Daten auf Systemen des Dienstleisters .....	8
7.1. Datenverarbeitung in Europa .....	8

7.2.	Zutrittsschutz .....	8
7.3.	Prozess zur Benutzerverwaltung.....	8
7.4.	Virenschutz .....	8
7.5.	Patchmanagement und Schwachstellenmanagement .....	8
7.6.	Datensicherungen .....	9
7.7.	Netzwerk.....	9
7.8.	Regelungen zu Clear-Screen und Clean-Desk.....	9
7.9.	Verfügbarkeit und Notfallmanagement.....	9
7.10.	Protokollierung.....	9
8.	Sicherheitsanforderungen für durchzuführende Entwicklungsleistungen.....	9
8.1.	Richtlinie zur sicheren Entwicklung .....	9
8.2.	Sichere Ablage von Quellcode .....	10
8.3.	Prüfung durch Tests.....	10
8.4.	Betriebskonzept zum sicheren Betrieb Software-Anwendung.....	10
8.5.	Schwachstellenmanagement.....	10
9.	Kontaktdaten.....	11
9.1.	Informationssicherheit .....	11
9.2.	Datenschutz .....	11
10.	Bestätigung durch den Auftragnehmer .....	11

## 1. Änderungshistorie

Version	Datum	Geänderte Kapitel	Grund der Änderung	Geändert durch
0.1	27.10.2025	Alle	Initiale Erstellung	tk
0.2	27.05.2026	Alle	Formale Anpassungen	zd
0.3	01.06.2026	10	Ergänzung	zd

## 2. Einleitung und Geltungsbereich

Dieses Dokument enthält die Sicherheitsanforderungen der Flughafen Hannover-Langenhagen GmbH (FHG) für Auftragnehmer zur Umsetzung der Dienstleistersteuerung gemäß ISO/IEC 27001:2022. Verbindlich sind ausschließlich die im Vertrag schriftlich vereinbarten Sicherheitsanforderungen.

Sollten einzelne Sicherheitsanforderungen nicht oder nur eingeschränkt umsetzbar sein, sind kompensatorische Maßnahmen zu vereinbaren und schriftlich zu dokumentieren. Die Kompensationsmaßnahmen müssen ein gleichwertiges Sicherheitsniveau aufweisen.

Zertifikate anerkannter Stellen (z. B. ISO/IEC 27001) können als Nachweis für die Erfüllung einzelner oder mehrerer Sicherheitsanforderungen dienen. Die Gültigkeit und Anwendbarkeit der Zertifikate wird durch die FHG geprüft.

## 3. Allgemeine Sicherheitsanforderungen

Unabhängig von Art und Umfang der erbrachten Leistungen gelten die nachfolgenden allgemeinen Sicherheitsanforderungen, die vom Auftragnehmer einzuhalten sind.

### 3.1. *Umgang mit Informationen des Auftraggebers*

Alle Informationen, die dem Auftraggeber zuzuordnen sind (entweder, weil diese vom Auftraggeber bereitgestellt wurden oder in dessen Auftrag erstellt wurden), sind vertraulich zu behandeln. Bei der Verarbeitung sind folgende Regelungen einzuhalten:

#### 3.1.1. Zugriffssteuerung

Der Bearbeiter- und Leserkreis ist nach dem Need-to-Know-Prinzip einzuschränken. Der Auftraggeber behält sich das Recht vor, die Zugriffsberechtigungen jederzeit einzusehen und zu überprüfen. Der Auftragnehmer hat auf Anforderung binnen fünf Werktagen eine aktuelle Übersicht der zugriffsberechtigten Personen bereitzustellen.

#### 3.1.2. Übertragungswege

- **Elektronisch:** Die elektronische Weitergabe von Informationen des Auftraggebers ist ausschließlich verschlüsselt zulässig. Dies gilt sowohl für die Übertragung im internen Netzwerk des Auftragnehmers als auch für die Übertragung über öffentliche Netzwerke (Internet). Es ist eine Verschlüsselung nach aktuellem Stand der Technik zu verwenden (mindestens TLS 1.2 oder vergleichbar).
- **Physisch:** Eine nicht-elektronische Weitergabe außerhalb der Geschäftsräume des Auftragnehmers erfolgt ausschließlich in verschlossenen Umschlägen oder Behältern. Eine Übertragung per Fax ist nicht zulässig.

### 3.1.3. Ablage und Aufbewahrung

- **Elektronisch:** Die Speicherung von Informationen des Auftraggebers auf mobilen Endgeräten (z. B. Laptops, Tablets, Smartphones) und Wechseldatenträgern (z. B. USB-Sticks, externe Festplatten) ist ausschließlich in verschlüsselter Form zulässig. Die Verschlüsselung muss dem aktuellen Stand der Technik entsprechen.
- **Physisch:** Die physische Ablage von Dokumenten ist nur zulässig, wenn das Need-to-Know-Prinzip sichergestellt werden kann, beispielsweise durch abschließbare Schränke oder Räumlichkeiten. Dokumente dürfen nicht unbeaufsichtigt, offen zugänglich oder ungesichert auf Schreibtischen, in Postfächern oder allgemein zugänglichen Bereichen abgelegt werden.

### 3.1.4. Vernichtung und Entsorgung

Die sichere Vernichtung von Dokumenten und Datenträgern, die Informationen des Auftraggebers enthalten, muss durch den Auftragnehmer gewährleistet sein.

Vertrauliche und personenbezogene Informationen und Dokumente müssen mindestens der Sicherheitsstufe P-4 für Papier, O-4 für optische Datenträger und H-4 für magnetische Datenträger gemäß DIN 66399 entsprechen.

Wird ein externer Entsorgungsdienstleister beauftragt, muss die sichere Aufbewahrung von Datenträgern und Dokumenten bis zur Abholung durch den Dienstleister gewährleistet sein, beispielsweise durch den Einsatz abschließbarer Datenschutzbehälter.

## 3.2. *Meldung von Informationssicherheitsvorfällen*

Der Auftragnehmer verpflichtet sich, dem Auftraggeber aufgetretene oder vermutete Informationssicherheitsvorfälle unverzüglich zu melden, sofern Informationen, Systeme oder Dienstleistungen des Auftraggebers betroffen sind oder betroffen sein könnten.

### 3.2.1. Definition Informationssicherheitsvorfälle

Als Informationssicherheitsvorfall gilt jedes Ereignis, bei dem die Schutzziele Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen des Auftraggebers beeinträchtigt wurden oder beeinträchtigt werden könnten. Dies umfasst insbesondere:

- Unbefugter Zugriff auf Informationen oder Systeme
- Verlust oder Diebstahl von Datenträgern oder Endgeräten
- Datenschutzverletzungen gemäß DSGVO
- Malware-Infektionen oder Cyberangriffe
- Systemausfälle, die die vereinbarten Verfügbarkeitsanforderungen überschreiten
- Unbeabsichtigte Offenlegung vertraulicher Informationen
- Verdacht auf Kompromittierung von Zugangsdaten

### 3.2.2. Meldepflicht und Meldefristen

Die Meldung eines Informationssicherheitsvorfalls hat unverzüglich, spätestens jedoch binnen 24 Stunden nach Kenntniserlangung, an die in Abschnitt 9 dieser Anlage genannten Kontaktstellen des Auftraggebers zu erfolgen.

### **3.2.3. Zu meldende Informationen**

Der Auftragnehmer übermittelt im Rahmen der Erstmeldung mindestens folgende Informationen:

- Zeitpunkt der Feststellung und vermuteter Zeitpunkt des Eintritts des Vorfalls
- Beschreibung der Art und des Umfangs des Informationssicherheitsvorfalls
- Kategorien und ungefähre Anzahl der betroffenen Informationen, Datensätze oder Systeme
- Name und vollständige Kontaktdaten eines Ansprechpartners für weitere Informationen und Koordination
- Beschreibung der wahrscheinlichen Folgen und möglichen Auswirkungen des Vorfalls
- Beschreibung der bereits ergriffenen Sofortmaßnahmen zur Eindämmung, Behebung oder Abmilderung des Vorfalls

### **3.3. *Sensibilisierung und Verpflichtung der Mitarbeiter***

Der Auftragnehmer verpflichtet sich, alle Mitarbeiter regelmäßig zur Informationssicherheit und zum Datenschutz zu sensibilisieren. Die Sensibilisierung der für den Auftraggeber tätigen Mitarbeiter umfasst dabei insbesondere die in diesem Dokument festgelegten vertraglichen Sicherheitsanforderungen.

Alle Mitarbeiter des Auftragnehmers, die Zugang zu Informationen des Auftraggebers haben oder haben könnten, werden vor Aufnahme ihrer Tätigkeit schriftlich auf Verschwiegenheit und das Datengeheimnis verpflichtet. Diese Verpflichtung muss auch über die Beendigung der Tätigkeit hinaus fortbestehen.

### **3.4. *Durchführung von Dienstleister-Audits***

Um die Einhaltung der geltenden Regelungen aus diesem Dokument sicherstellen zu können, führt die FHG regelmäßige und anlassbezogene Überprüfungen durch. Die Überprüfungen können in folgenden Formen durchgeführt werden:

- Einreichung gültiger Zertifikate (z. B. ISO/IEC 27001), die eine ausreichende Abdeckung der in diesem Dokument festgelegten Sicherheitsanforderungen belegen.
- Bereitstellung von Sicherheitsdokumenten, Richtlinien und Verfahrensbeschreibungen in digital durchsuchbarer Form.
- Durchführung von Vor-Ort-Audits in Räumlichkeiten des Auftragnehmers bei begründetem Verdacht auf Nichteinhaltung der Sicherheitsanforderungen. Vor-Ort-Audits werden angekündigt und folgen einem vorab zwischen den Parteien abgestimmten Auditplan.
- Durchführung von Interviews per Videokonferenz oder Telefon zur Überprüfung der Umsetzung von Sicherheitsmaßnahmen.

Die Bereitstellung von Unterlagen, Zertifikaten und Nachweisen erfolgt kostenfrei durch den Auftragnehmer. Bei Vor-Ort-Audits trägt die FHG die Kosten für eigene Auditoren oder beauftragte externe Prüfer. Der Auftragnehmer stellt kostenfrei geeignete Räumlichkeiten, Ansprechpartner und erforderliche Zugangsberechtigungen für die Durchführung der Audits bereit.

### **3.5. *Regelungen zum Ende der Tätigkeiten***

Bei Beendigung des Vertragsverhältnisses müssen alle vom Auftraggeber ausgegebenen Unterlagen, Daten, IT-Systeme, Geräte sowie erstellte Arbeitsergebnisse vollständig an den Auftraggeber übergeben werden. Die Rückgabe hat spätestens am letzten Tag der Leistungserbringung zu erfolgen.

Alle Informationen und Daten des Auftragnehmers, die auf IT-Systemen, mobilen Endgeräten, Wechseldatenträgern, Backup-Systemen oder sonstigen Speichermedien des Auftragnehmers gespeichert wurden, sind nach Beendigung des Vertragsverhältnisses vollständig und sicher zu löschen. Die Löschung muss dem aktuellen Stand der Technik entsprechen und gewährleisten, dass die Daten nur mit erheblichem Aufwand wiederherstellbar sind. Der Auftragnehmer hat nach Beendigung des Vertragsverhältnisses einen schriftlichen Nachweis über die vollständige und sichere Löschung aller Daten des Auftragnehmers zu erbringen.

Alle dem Auftragnehmer oder dessen Mitarbeitern gewährten Zutritts- und Zugangsberechtigungen (physisch und logisch) werden mit sofortiger Wirkung bei Beendigung des Vertragsverhältnisses gesperrt.

### **3.6.      *Weitergabe der Sicherheitsanforderungen an Unterauftragnehmer***

Der Auftragnehmer ist verpflichtet, die in diesem Dokument festgelegten Informationssicherheitsanforderungen vollständig und unverändert an alle eigenen Lieferanten und Unterauftragnehmer weiterzugeben, sofern diese zur Leistungserbringung für den Auftraggeber eingesetzt werden oder Zugang zu Informationen des Auftraggebers haben.

Der Auftragnehmer ist verpflichtet, den Auftraggeber vor dem Einsatz neuer Unterauftragnehmer oder bei wesentlichen Änderungen bezüglich der bereits eingesetzten Unterauftragnehmer (z. B. Wechsel, Erweiterung des Leistungsumfangs, Änderung der Standorte) schriftlich zu informieren.

Die Einhaltung der weitergegebenen Sicherheitsanforderungen durch die Unterauftragnehmer liegt im Verantwortungsbereich des Auftragnehmers.

## **4. Sicherheitsanforderungen für Arbeiten mit Systemen des Auftraggebers**

### **4.1.      *Arbeiten an IT-Systemen***

Erhält der Auftragnehmer Clients des Auftraggebers zur Nutzung ausgehändigt, sind diese gemäß der ISMS-Endbenutzerrichtlinie der FHG zu verwenden. Die Regelungen der ISMS-Endbenutzerrichtlinie sind verbindlich einzuhalten.

### **4.2.      *Umgang mit Clients des Auftraggebers***

Arbeiten an IT-Systemen des Auftraggebers sind ausschließlich mit zugelassenen Clients erlaubt.

Zugelassene Clients umfassen vom Auftraggeber ausgegebene Clients sowie angemessen geschützte Clients des Auftragnehmers, die den aktuellen Stand der Technik hinsichtlich Patchmanagement und Virenschutz aufweisen.

### **4.3.      *Umgang mit Zugangsdaten***

Zugänge zu Systemen des Auftraggebers sind durch Passwörter zu schützen, die die Anforderungen der Passwortrichtlinie aus der ISMS-Endbenutzerrichtlinie der FHG erfüllen. Die Weitergabe von Zugangsdaten an Dritte ist untersagt.

## **5. Besondere Sicherheitsanforderungen für Arbeiten an IT-Systemen innerhalb der Räumlichkeiten des Auftraggebers**

Für Arbeiten an IT-Systemen innerhalb der Räumlichkeiten des Auftraggebers gelten die Regelungen der ISMS-Endbenutzerrichtlinie der FHG.

### **5.1. Zugang zu Remote-Systemen**

Remote-Verbindungen dürfen ausschließlich über die vom Auftraggeber bereitgestellte Anwendung aufgebaut werden. Wurde für die Remote-Verbindungen ein Client des Auftraggebers ausgehändigt, darf nur dieser eingesetzt werden.

Die vorkonfigurierten Sicherheitseinstellungen, Zertifikatsdateien oder Verbindungsparameter dürfen nicht verändert werden.

Der Auftragnehmer kündigt die Durchführung geplanter Arbeiten über die Remote-Verbindung im Vorfeld beim zuständigen Ansprechpartner des Auftraggebers an. Bei ungeplanten Arbeiten ist der Auftraggeber nach Möglichkeit im Vorfeld zu informieren. Falls dies nicht möglich ist, sind die durchgeführten Arbeiten zu dokumentieren und dem Auftraggeber unverzüglich mitzuteilen.

### **5.2. Umgang mit Remote-Zugangsdaten**

Für den Umgang mit Remote-Zugangsdaten gelten die Anforderungen der ISMS-Endbenutzerrichtlinie der FHG.

### **5.3. Protokollierung der Tätigkeiten**

Durchgeführte Tätigkeiten über Remote-Verbindungen sind vom Auftragnehmer zu dokumentieren, beispielsweise durch einen Tätigkeitsbericht oder in Form abgearbeiteter Tickets.

Der Auftraggeber behält sich das Recht vor, die über Remote-Verbindungen durchgeführten Tätigkeiten automatisiert aufzuzeichnen und zu protokollieren.

## **6. Sicherheitsanforderungen für Arbeiten an Systemen in Räumlichkeiten des Auftragnehmers**

Diese Anforderungen gelten, wenn Systeme des Auftraggebers für Reparatur- oder Wartungsarbeiten vorübergehend in Räumlichkeiten des Auftragnehmers aufbewahrt und genutzt werden.

### **6.1. Sichere Aufbewahrung**

Die Systeme des Auftraggebers müssen beim Auftragnehmer sicher verwahrt werden und dürfen nur den Mitarbeitern zugänglich sein, die tatsächlich an den Systemen arbeiten müssen.

Wenn Daten des Auftraggebers temporär auf anderen Systemen oder Datenträgern gespeichert werden müssen, sind diese verschlüsselt zu übertragen und zu speichern.

### **6.2. Sicherer Transport**

Auch während des Transports müssen die Systeme des Auftraggebers sicher aufbewahrt werden und dürfen nicht unbeaufsichtigt gelassen werden.



### **6.3.      *Protokollierung der Tätigkeiten***

Durchgeführte Tätigkeiten sind vom Auftragnehmer durch einen Tätigkeitsbericht oder Auftragsbestätigungen zu dokumentieren.

## **7. Sicherheitsanforderungen für die Verarbeitung von Daten auf Systemen des Dienstleisters**

Die nachfolgenden Anforderungen gelten, wenn der Auftragnehmer Daten des Auftraggebers auf seinen eigenen Systemen verarbeitet. Alternativ kann der Auftragnehmer technisch-organisatorische Maßnahmen zur Prüfung einreichen.

### **7.1.      *Datenverarbeitung in Europa***

Die Datenverarbeitung findet ausschließlich in Europa statt und wird auf dem Transportweg vor unbefugter Einsichtnahme geschützt.

### **7.2.      *Zutrittsschutz***

Die Verarbeitung der Daten muss in zugriffsgeschützten Bereichen stattfinden. Die Zutrittsrechte werden gemäß dem Need-to-Know-Prinzip eingeschränkt vergeben. Der Vergabeprozess muss klar definiert und dokumentiert sein. Vergabene Zutrittsberechtigungen müssen mindestens jährlich auf ihre Aktualität geprüft werden.

Die Bereiche müssen angemessen gegen unbefugte Zutritte und Einbrüche geschützt werden. Bei der Verarbeitung von vertraulichen Daten sollte beispielsweise eine Einbruchmeldeanlage oder vergleichbare Schutzmaßnahme umgesetzt sein.

### **7.3.      *Prozess zur Benutzerverwaltung***

Der Zugang zu den datenverarbeitenden Systemen muss gemäß dem Need-to-Know-Prinzip eingeschränkt vergeben werden. Der Vergabeprozess muss klar definiert und dokumentiert sein. Vergabene Zugänge müssen mindestens jährlich auf Aktualität geprüft werden.

### **7.4.      *Virenschutz***

Auf den eingesetzten Systemen zur Datenverarbeitung muss entweder ein Anti-Viren-Programm installiert oder analysiert und dokumentiert worden sein, warum auf einen Virenschutz verzichtet werden kann.

Wenn Anti-Viren-Programme eingesetzt werden, müssen die Viren-Pattern mindestens täglich aktualisiert werden. Es muss sichergestellt werden, dass Virenfunde zentral ausgewertet werden können.

### **7.5.      *Patchmanagement und Schwachstellenmanagement***

Für die betrieblichen Systeme muss ein angemessenes Patch- und Schwachstellenmanagement betrieben werden. Dies umfasst insbesondere ein Prüf- und Freigabeverfahren, wenn durch Updates die Dienstleistung für den Auftraggeber gefährdet sein könnte.

Sicherheitskritische Updates werden unverzüglich auf allen betroffenen Systemen installiert oder es werden mitigierende Maßnahmen zur Reduzierung des Sicherheitsrisikos bis zur Installation der Updates umgesetzt.



## **7.6.      *Datensicherungen***

Der Auftragnehmer muss ein angemessenes Verfahren zur Datensicherung etabliert haben. Falls Datenverluste die erbrachte Datenverarbeitung für den Auftraggeber gefährden könnten, sollten Datensicherungen mindestens täglich erstellt und mindestens eine Woche aufbewahrt werden. Außerdem müssen regelmäßig Wiederherstellungstests durchgeführt werden.

## **7.7.      *Netzwerk***

Die datenverarbeitenden Systeme werden in einem segmentierten Netz betrieben und der Zugang ist gemäß dem Need-to-Know-Prinzip gesichert.

Das Netzwerk wird durch eine Firewall geschützt und die Firewall-Regeln werden mindestens jährlich auf ihre Korrektheit geprüft. Die Prüfung der Regeln wird gegenüber dem Auftraggeber nachgewiesen.

Der externe Zugang zu den Systemen ist angemessen abgesichert, beispielsweise durch VPN-Zugänge.

## **7.8.      *Regelungen zu Clear-Screen und Clean-Desk***

Die Anforderungen ergeben sich aus der ISMS-Endbenutzerrichtlinie der FHG.

## **7.9.      *Verfügbarkeit und Notfallmanagement***

Der Auftragnehmer muss angemessene Maßnahmen treffen, um die vertraglich zugesicherten Verfügbarkeiten der Datenverarbeitungen gewährleisten zu können.

## **7.10.    *Protokollierung***

Die Ereignisse auf den IT-Systemen und Netzwerkkomponenten sollten protokolliert und regelmäßig geprüft werden. Die Aufbewahrung sollte angemessen abgesichert sein, um Veränderungen durch Dritte zu verhindern bzw. aufdecken zu können.

Insbesondere sollten die Zugriffe auf Daten des Auftraggebers nachvollziehbar dokumentiert werden.

# **8. Sicherheitsanforderungen für durchzuführende Entwicklungsleistungen**

Die nachfolgenden Anforderungen gelten, wenn der Auftragnehmer Entwicklungsdienstleistungen für den Auftraggeber durchführt.

## **8.1.      *Richtlinie zur sicheren Entwicklung***

Der Auftragnehmer verfügt über eine Richtlinie zur sicheren Entwicklung. Bestandteil der Richtlinie sind Regelungen zum sicheren Einsatz notwendiger Frameworks und Bibliotheken, Vorgaben zur Verhinderung und Mitigation bekannter Schwachstellen (z. B. OWASP Top Ten) und Verfahren, um die Anwendung und Wirksamkeit der Richtlinie zu gewährleisten (z. B. Code Reviews, Pair-Programming oder vergleichbare Maßnahmen).

## **8.2. Sichere Ablage von Quellcode**

Der Quellcode für entwickelte Software-Produkte ist in gesicherten Repositories aufzubewahren. Der Zugriff auf die Repositories ist nach dem Need-to-Know-Prinzip zu vergeben, um unbefugte Änderungen zu verhindern.

Das Repository sollte eine automatisierte Versionskontrolle und Sicherung des Quellcodes ermöglichen.

## **8.3. Prüfung durch Tests**

Der Auftragnehmer testet während der Entwicklung die funktionalen und sicherheitstechnischen Anforderungen.

## **8.4. Betriebskonzept zum sicheren Betrieb Software-Anwendung**

Der Auftragnehmer verpflichtet sich, ein Betriebskonzept zum sicheren Betrieb der entwickelten Software vorzulegen.

Dieses Konzept sollte dabei folgende Aspekte (wenn relevant) enthalten:

- Rollen- und Berechtigungskonzept
- Backups
- Verschlüsselung
- Patching

## **8.5. Schwachstellenmanagement**

Der Auftragnehmer verpflichtet sich, dem Auftraggeber identifizierte sicherheitskritische Schwachstellen in den betreuten Anwendungen unverzüglich zu melden. Schwachstellen werden vom Auftragnehmer untersucht und behoben. Der Auftraggeber wird regelmäßig über die Behandlung der Schwachstelle und den Status des dazugehörigen Updates informiert.

Der Auftragnehmer wird im Rahmen der Meldung aufgetretener Schwachstellen dem Auftraggeber mindestens folgende Informationen mitteilen:

- Eine Beschreibung der Schwachstellen;
- Name und Kontaktdaten eines Ansprechpartners für weitere Informationen;
- Eine Beschreibung der geplanten Maßnahmen zur Behebung und der voraussichtliche Zeitplan zur Bereitstellung der dazugehörigen Updates.

Der Auftragnehmer hat ein Schwachstellenmanagement etabliert, das die kontinuierliche Anpassung etablierter Regelungen und Vorgaben sowie die Sensibilisierung und Weiterbildung der Mitarbeiter gegenüber neu identifizierten Schwachstellen sicherstellt, um die Wahrscheinlichkeit zur Wiederholung der Schwachstellen zu minimieren.

## 9. Kontaktdaten

Bei Fragen zu Anforderungen oder zur Meldung von Vorfällen können Sie sich an folgende Personen wenden.

### 9.1. Informationssicherheit

- Name: Zeynep Demir
- E-Mail: z.demir@hannover-airport.de
- Telefon: +49 (0)173 9971599

### 9.2. Datenschutz

- Name: Marion Kutscha
- E-Mail: m.kutscha@hannover-airport.de
- Telefon: +49 (0)173 9971420

## 10. Bestätigung durch den Auftragnehmer

Der Auftragnehmer bestätigt mit seiner Unterschrift, dass er die vorstehenden Informationssicherheitsanforderungen gelesen und verstanden hat. Der Auftragnehmer verpflichtet sich, die Anforderungen im Rahmen der beauftragten Leistungen einzuhalten und die Einhaltung auch bei eingesetzten Mitarbeitern sowie, soweit zutreffend, Unterauftragnehmern sicherzustellen.

<b>Auftragnehmer</b>		<b>Kontakt</b>	
<b>Ort</b>		<b>Datum</b>	
<b>Unterschrift</b>			
<i>Hinweis: Die Unterzeichnung ersetzt keine gesonderten vertraglichen Vereinbarungen, sondern dokumentiert die Kenntnisnahme und Verpflichtung zur Einhaltung dieser Anlage.</i>			