1 Governance und Richtlinien /Guidelines:

1.1 ISMS

The effectiveness of the ISMS must be reviewed and verified through regular audits. The CONTRACTUAL PARTNER undertakes to implement all necessary corrective and preventive measures in a timely manner in order to ensure the continuous improvement of information security management.	Die Effektivität des ISMS muss durch regelmäßige Audits überprüft und nachgewiesen werden. Der VERTRAGSPARTNER verpflichtet sich, alle erforderlichen Korrektur- und Vorbeugemaßnahmen zeitnah umzusetzen, um die kontinuierliche Verbesserung des Informationssicherheitsmanagements zu gewährleisten.

1.2 GUIDELINES RICHTLINIEN

Information security policies, procedures, roles and responsibilities are defined. The information security policies are approved by the management, published and communicated to employees and relevant external parties.	Informationssicherheitsrichtlinien, -verfahren, -rollen, -verantwortlichkeiten sind festgelegt. Die Informationssicherheitsrichtlinien werden von der Geschäftsleitung genehmigt, veröffentlicht und an die Mitarbeiter*innen, sowie relevante externe Parteien kommuniziert.
The CONTRACTUAL PARTNER shall regularly review its compliance with the established information security policies and standards and all other relevant and contractual security requirements.	Der VERTRAGSPARTNER überprüft regelmäßig, ob er die festgelegten Informationssicherheitsrichtlinien und -standards sowie alle anderen relevanten und vertraglichen Sicherheitsanforderungen einhält.

1.3 RISK MANAGEMENT RISIKOMANAGEMENT

The CONTRACTUAL PARTNER shall ensure that risks that could have a direct or indirect impact on the services and data (e.g. loss of reputation, data, revenue, etc.) are assessed and appropriate mitigation measures are implemented and documented. Upon request or in the event of direct effects for the client, these must be reported to the client.	Der VERTRAGSPARTNER stellt sicher, dass Risiken, die sich direkt oder indirekt auf die Services und Daten auswirken (bspw. Verlust von Reputation, Daten, Umsatz etc.) könnten, bewertet und entsprechende Minderungsmaßnahmen umgesetzt sowie dokumentiert werden. Bei Aufforderung oder bei unmittelbaren Auswirkungen für den Auftraggeber sind diese an den Auftraggeber zu melden.

1.4 BUSINESS CONTINUITY MANAGEMENT

CONTRACTUAL PARTNER shall have up-to-date and maintained disaster recovery plans and business continuity plans. The disaster recovery plans and business continuity plans shall be designed to minimize the negative impact of unplanned interruptions and to ensure that the CONTRACTUAL PARTNER can continue to operate and provide the services in accordance with the contract with the CLIENT even in the event of business interruptions.	VERTRAGSPARTNER verfügt über aktuelle und aufrechterhaltene Notfallpläne und Pläne zur Aufrechterhaltung des Geschäftsbetriebs. Die Desaster-Recovery-Pläne und Business-Continuity-Pläne müssen so konzipiert sein, dass negative Auswirkungen durch ungeplante Unterbrechungen so weit wie möglich verhindert werden und dass der VERTRAGSPARTNER auch bei Betriebsunterbrechungen weiterarbeiten und die Dienstleistungen gemäß dem Vertrag mit dem KUNDEN erbringen kann.
The CONTRACTUAL PARTNER conducts appropriate testing of its own business continuity and disaster recovery plans.	Der VERTRAGSPARTNER führt angemessene Tests seiner eigenen Business Continuity- und Desaster-Recovery-Pläne durch.
The CONTRACTUAL PARTNER has ensured that the scope of the business continuity and disaster recovery plans covers all sites, employees and information systems used to provide services to the CLIENT.	Der VERTRAGSPARTNER hat sichergestellt, dass der Geltungsbereich der Business Continuity- und Notfallwiederherstellungspläne alle Standorte, Mitarbeiter*innen und Informationssysteme umfasst, die zur Erbringung von Dienstleistungen für den KUNDEN eingesetzt werden.

1.5 IDENTITY & ACCESSMANAGEMENT

IDENTITÄTS- UND ZUGRIFFSMANAGEMENT

The CONTRACTUAL PARTNER has set up access controls to verify identities and restrict access to authorized users. Access rights are based on the "need to know principle" and the "least privilege principle". In addition, the principle of "separation of functions" is observed.	Der VERTRAGSPARTNER hat Zugangskontrollen eingerichtet, um Identitäten zu überprüfen und den Zugang auf autorisierte Benutzer zu beschränken. Die Zugriffsrechte beruhen auf den Grundsätzen "Need To Know Prinzip" und "Least Privilege Prinzip". Darüber hinaus wird der Grundsatz der "Funktionstrennung" beachtet.
The CONTRACTUAL PARTNER has implemented authentication mechanisms to protect access to the systems in accordance with best practice, including the following: -Password guidelines (minimum length, complexity, avoidance of reuse) -Unique user identification (generic and shared users are avoided) -secure storage/management/ transmission of credentials	Der VERTRAGSPARTNER hat Authentifizierungsmechanismen implementiert, um den Zugang zu den Systemen nach bewährten Verfahren zu schützen, die unter anderem Folgendes umfassen: -Passwortrichtlinien (Mindestlänge, Komplexität, Vermeidung von Wiederverwendung) eindeutige Benutzeridentifikation (generische und gemeinsame Benutzer werden vermieden) -Sichere Speicherung/Verwaltung/ Übermittlung von Anmeldedaten
The CONTRACTUAL PARTNER shall ensure that accounts used for access via the Internet are protected by strong authentication mechanisms (e.g. multi-factor authentication).	Der VERTRAGSPARTNER stellt sicher, dass Konten, die für den Zugang über das Internet genutzt werden, durch starke Authentifizierungsmechanismen (bspw. Multi-Faktor Authentifizierung) geschützt werden.
The CONTRACTUAL PARTNER has implemented strict controls for privileged accounts (e.g. system administrators) through strong authentication, restriction to a minimum and strictly monitored usage (e.g. logging).	Der VERTRAGSPARTNER hat strenge Kontrollen für privilegierte Konten (z.B. Systemadministratoren) durch starke Authentifizierung, Beschränkung auf ein Minimum und streng überwachte Nutzung (z. B. Protokollierung) eingeführt.
The CONTRACTUAL PARTNER shall review the access rights of its employees at regular intervals and change (i.e. restrict/revoke) them if necessary. The CONTRACTUAL PARTNER has a controlled exit process for employees, which ensures the deactivation or deletion of accounts provided by them.	Der VERTRAGSPARTNER überprüft die Zugriffsrechte seiner Mitarbeiter*innen in regelmäßigen Abständen und ändert (d.h. beschränkt/widerruft) sie, falls erforderlich. Der Vertragspartner hat einen kontrollierten Austrittsprozess von Mitarbeitenden, welcher die Deaktivierung respektive Löschung mitliefernde Accounts sicherstellt.

1.6 AWARENESS SENSIBILISIERUNG

All employees of the CONTRACT PARTNER and, where applicable, the CONTRACTUAL PARTNERs shall receive awareness training on information security-related topics appropriate to their function. In addition, employees shall also be informed of updates to the CONTRACTUAL PARTNER's policies and procedures. Employees must have the knowledge required for their tasks and responsibilities.	Alle Mitarbeiter*innen des VERTRAGSPARTNERS und gegebenenfalls auch die Auftragnehmer erhalten eine ihrer Funktion entsprechende Sensibilisierung bzgl. Informationssicherheitsrelevanter Themen. Darüber hinaus werden die Mitarbeiter*innen auch über Aktualisierungen der Richtlinien und Verfahren des VERTRAGSPARTNERs unterrichtet. Die Mitarbeiter*innen müssen, über die für die Aufgaben und Zuständigkeiten erforderlichen Kenntnisse verfügen.

1.7 CONTRACTUAL AGREEMENT VERTRAGLICHE VEREINBARUNG

The CONTRACTUAL PARTNER must include responsibility for information security in the contractual agreements with its employees and CONTRACTUAL PARTNERs.	Der VERTRAGSPARTNER muss die Verantwortung für die Informationssicherheit in die vertraglichen Vereinbarungen mit den Mitarbeiter*innen und Auftragnehmern aufnehmen.

1.8 SUB-OUTSOURCING

The CONTRACTUAL PARTNER shall have clear contractual arrangements with all Sub CONTRACTUAL PARTNERs of services to define their responsibility for the security of the DATA they process / store / transmit on behalf of the CLIENT. The CONTRACTUAL PARTNER shall ensure that the security measures implemented by the SUBCONTRACTUAL PARTNERS are at least at the level specified in this document and in the main contract.	Der VERTRAGSPARTNER hat klare vertragliche Vereinbarungen mit allen Unterauftragnehmern von Dienstleistungen, um deren Verantwortung für die Sicherheit der DATEN, die sie im Auftrag des KUNDEN verarbeiten / speichern / übermitteln, festzulegen. Der VERTRAGSPARTNER stellt sicher, dass die von den UNTERAUFTRAGNEHMERN eingeführten Sicherheitsmaßnahmen mindestens das in diesem Dokument und im Hauptvertrag angegebene Niveau haben.

2 Physische und Infrastruktur Sicherheit / Physical and Network Security:

2.1 PHYSICAL SECURITY PHYSISCHE SICHERHEIT

The CONTRACTUAL PARTNER has divided its premises into different protection zones, which reflect certain security measures and access rights according to the respective security requirements (e.g. network infrastructure, offices).	Der VERTRAGSPARTNER hat seine Räumlichkeiten in verschiedene Schutzzonen eingeteilt, die bestimmte Sicherheitsmaßnahmen und Zugangsrechte entsprechend den jeweiligen Sicherheitsanforderungen widerspiegeln (z.B. Netzwerk-Infrastruktur, Büroräume).
Access to IT systems such as servers is further restricted by special protection zones that are only accessible to authorized personnel.	Der Zugang zu IT-Systemen wie z.B. Servern ist durch spezielle Schutzzonen, die nur für befugtes Personal zugänglich sind, weiter eingeschränkt.

2.2 NETWORK SECURITY

The CONTRACTUAL PARTNER has implemented and maintained network security infrastructure components such as firewalls, intrusion detection/prevention systems (IDS/IPS) and other security controls in accordance with its protection requirements, which enable detection, continuous monitoring and restriction of network traffic in order to limit the impact of attacks. For systems with a higher risk level (e.g. accessible from external networks), more stringent measures must be taken.	Der VERTRAGSPARTNER hat Komponenten der Netzsicherheitsinfrastruktur wie Firewalls, Intrusion Detection/Prevention Systeme (IDS/IPS) und andere Sicherheitskontrollen entsprechend seinem Schutzbedarf implementiert und aufrechterhalten, die eine Erkennung, kontinuierliche Überwachung und eine Einschränkung des Netzwerk Traffics ermöglichen, um die Auswirkungen von Angriffen zu begrenzen. Für Systeme mit einer höheren Risikostufe (z.B. für einen Zugriff von externen Netzwerken erreichbar) müssen strengere Maßnahmen ergriffen werden.
The CONTRACTUAL PARTNER has established a policy for remote access that specifies the circumstances under which administrative activities are carried out remotely on the systems provided by the CONTRACTUAL PARTNER, for example to rectify faults or to carry out necessary maintenance work. This policy is intended to ensure that such interventions only take place under defined and controlled conditions.	Der VERTRAGSPARTNER hat eine Richtlinie für Fernzugriffe etabliert, die festlegt, unter welchen Umständen administrative Tätigkeiten an den von ihm bereitgestellten Systemen aus der Ferne durchgeführt werden, etwa zur Behebung von Störungen oder zur Durchführung erforderlicher Wartungsarbeiten. Diese Richtlinie soll gewährleisten, dass solche Eingriffe nur unter definierten und kontrollierten Bedingungen erfolgen.
The CONTRACTUAL PARTNER shall ensure the separation and segmentation of environments in accordance with industry standards if: (1) environments are shared with other CLIENTs; and/or (2) the CONTRACTUAL	Der VERTRAGSPARTNER stellt die Trennung und Segmentierung der Umgebungen gemäß Industriestandards sicher, wenn: (1) Umgebungen gemeinsam mit anderen Kunden genutzt werden; und/oder (2) der

PARTNER establishes test, quality and production environments.	VERTRAGSPARTNER Test-, Qualitäts- und Produktionsumgebungen einrichtet.

3 Daten- und Anwendungssicherheit / Application Security: Data and

3.1 ASSET MANAGEMENT / LIFECYCLE

The CONTRACTUAL PARTNER shall ensure that information security is an integral part of the information systems over their entire life cycle (acquisition/development to decommissioning of the systems, applications and facilities). The relevant assets are maintained in a central register. The CONTRACTUAL PARTNER shall ensure that the software provided is supported by operating systems and middleware (e.g. Java) versions that receive security updates and are not at the end of their life cycle. The CONTRACTUAL PARTNER shall provide regular and timely security updates throughout the contract lifecycle.	Der VERTRAGSPARTNER stellt sicher, dass die Informationssicherheit ein integraler Bestandteil der Informationssysteme über deren gesamten Lebenszyklus ist (Erwerb/Entwicklung bis Stilllegung der Systeme, Applikationen und Anlagen). Die relevanten Assets werden in einem zentralen Register gepflegt. Der VERTRAGSPARTNER stellt sicher, dass die bereitgestellte Software von Betriebssystemen und Middleware (z.B. Java) Versionen unterstützt wird, die Sicherheitsupdates erhalten und nicht am Ende ihres Lebenszyklus stehen. Der VERTRAGSPARTNER liefert regelmäßige und rechtzeitige Sicherheitsupdates über den gesamten Vertragslebenszyklus hinweg.

3.2 SECURE SOTWARE DEVELOPMENT LIFECYCLE LEBENSZYKLUS DER SICHEREN SOFTWAREENTWICKLUNG

The CONTRACTUAL PARTNER shall include information security aspects in the product documentation. This documentation shall include instructions for the configuration of the service and/or environment to ensure secure operation. Developed software must be tested in a controlled environment to identify vulnerabilities before it is made available.	Der VERTRAGSPARTNER nimmt Aspekte der Informationssicherheit in die Produkt-dokumentation auf. Diese Dokumentation muss Anweisungen für die Konfiguration des Dienstes und/oder der Umgebung enthalten, um einen sicheren Betrieb zu gewährleisten. Entwickelte Software muss in einer kontrollierten Umgebung getestet werden, um Schwachstellen zu erkennen, bevor sie zur Verfügung gestellt wird.
The CONTRACTUAL PARTNER shall ensure that the software development lifecycle contains appropriate security measures (Secure Software Development Lifecycle). The CONTRACTUAL PARTNER commits to secure development practices based on international standards (such as OWASP) to ensure the overall security of the software. This includes ongoing code reviews through static and dynamic security tests and vulnerability scans that also include external and open source components.	Der VERTRAGSPARTNER stellt sicher, dass der Lebenszyklus der Softwareentwicklung angemessene Sicherheitsmaßnahmen enthält (Secure Software Development Lifecycle). Der VERTRAGSPARTNER verpflichtet sich zu sicheren Entwicklungspraktiken (wie bspw. OWASP), die auf internationalen Standards basieren, um die allgemeine Sicherheit der Software zu garantieren. Dies umfasst fortlaufende Überprüfungen des Codes durch statische und dynamische Sicherheitstests sowie Schwachstellen-Scans, die auch externe und Open-Source-Komponenten einbeziehen.

3.3 SOFTWARE CHANGEMANAGEMENT

The CONTRACTUAL PARTNER has formal guidelines for change management and the life cycle of secure software development, which also define security-related controls. Information security reviews of new system designs or changes to systems must be part of the processes. Changes are appropriately requested, authorized, tested and approved before they are released for production.	Der VERTRAGSPARTNER verfügt über formale Richtlinien für das Change-Management und den Lebenszyklus der sicheren Softwareentwicklung, die auch sicherheitsrelevante Kontrollen festlegen. Überprüfungen der Informationssicherheit bei neuen Systemdesigns oder Änderungen an Systemen müssen Teil der Prozesse sein. Änderungen werden in angemessener Weise

	angefordert, autorisiert, getestet und genehmigt, bevor sie für die Produktion freigegeben werden.

3.4 DATA MANAGEMENT

The CONTRACTUAL PARTNER shall ensure that measures are taken against data loss and leakage.	Der VERTRAGSPARTNER stellt sicher, dass Maßnahmen gegen Datenverlust und -abfluss getroffen werden.
The CONTRACTUAL PARTNER shall not replicate or use the CLIENT's production data in non-production environments. Any use of CLIENT data in non-production environments requires the express, documented consent of the CLIENT.	Der VERTRAGSPARTNER darf keine Produktionsdaten des KUNDEN replizieren oder in Nicht-Produktionsumgebungen verwenden. Jede Verwendung von Kundendaten in Nicht-Produktionsumgebungen bedarf der ausdrücklichen, dokumentierten Zustimmung des KUNDEN.

3.5 ENCRYPTION VERSCHLÜSSELUNG

The CONTRACTUAL PARTNER shall ensure adequate protection of the confidentiality of the data. The CONTRACTUAL PARTNER shall also consider specific measures for data in transit and in volatile and persistent storage, such as the use of encryption technologies in combination with an appropriate key management architecture. Encryption shall comply with leading standards and guidelines or equivalent standards (e.g. National Institute of Standards and Technology - NIST)	Der VERTRAGSPARTNER gewährleistet einen angemessenen Schutz der Vertraulichkeit der Daten. Der VERTRAGSPARTNER muss auch spezifische Maßnahmen für Daten bei der Übertragung sowie in flüchtigen und persistenten Speichertechnologien berücksichtigen, wie z. B. die Verwendung von Verschlüsselungstechnologien in Kombination mit einer geeigneten Schlüsselverwaltungs-Architektur. Die Verschlüsselung entspricht den führenden Standards und Richtlinien oder gleichwertigen Standards (bspw. National Institute of Standards and Technology - NIST)
The CONTRACTUAL PARTNER shall protect mobile devices and external electronic media (e.g. USB memory, tape) against unauthorized access by means of appropriate physical and logical security measures. The encryption of data stored on these devices must be enforced.	Der VERTRAGSPARTNER schützt mobile Geräte und externe elektronische Medien (z.B. USB-Speicher, Band) durch angemessene physische und logische Sicherheitsmaßnahmen vor unbefugtem Zugriff. Die Verschlüsselung von auf diesen Geräten gespeicherten Daten muss durchgesetzt werden.

4 Sicherheitsmanagement und Operation / Security Management and Operation:

4.1 SYSTEM HARDENING

The CONTRACTUAL PARTNER has configured and deployed its IT resources (e.g. databases, applications, operating systems, network devices) using a secure foundation (hardening). The security basis is based on best practices (e.g. CIS standards) or equivalent procedures. The configurations for the IT systems are regularly reviewed and updated.	Der VERTRAGSPARTNER hat seine IT-Ressourcen (z.B. Datenbanken, Anwendungen, Betriebssysteme, Netzwerkgeräte) unter Verwendung einer sicheren Grundlage (Hardening) konfiguriert und eingesetzt. Die Sicherheitsgrundlagen basieren auf Best Practices (z.B. CIS-Standards) oder gleichwertigen Verfahren. Die Konfigurationen für die IT-Anlagen werden regelmäßig überprüft und aktualisiert.

4.2 VULNERABILITY AND PATCH MANAGEMENT SCHWACHSTELLEN UND PATCH MANAGEMENT

The CONTRACTUAL PARTNER regularly analyses the systems (operating systems, applications, network components) for known vulnerabilities. Patches are applied in a consistent, standardized manner and prioritized according to their criticality. If the cause of	Der VERTRAGSPARTNER analysiert regelmäßig die Systeme (Betriebssysteme, Anwendungen, Netzkomponenten) auf bekannte Schwachstellen. Patches werden in einer konsistenten, standardisierten Weise angewendet und nach ihrer Kritikalität priorisiert.

vulnerabilities cannot be eliminated within a reasonable period of time, alternative measures must be taken to minimize the risk until they are eliminated. The CONTRACTUAL PARTNER has implemented an emergency change process.	Wenn die Ursache von Schwachstellen nicht innerhalb eines angemessenen Zeitraums beseitigt werden kann, müssen bis zur Behebung alternative Maßnahmen zur Risikominderung ergriffen werden. Der VERTRAGSPARTNER hat einen Notfall-Changeprozess implementiert.

4.3 PROTECTION AGAINST MALWARE SCHUTZ VOR SCHADSOFTWARE

The CONTRACTUAL PARTNER shall protect the servers and end devices with appropriate protection against malware, which shall always be kept up to date. The software must ensure that the anti-virus/malware software on the devices has not been deactivated and is regularly updated.	Der VERTRAGSPARTNER schützt die Server und Endgeräte mit einem angemessenen Schutz vor Malware, der stets auf dem neuesten Stand gehalten wird. Die Software muss sicherstellen, dass die Antiviren-/Malware-Software auf den Geräten nicht deaktiviert wurde und regelmäßig aktualisiert wird.

4.4 BACKUP & RECOVERY

The CONTRACTUAL PARTNER shall ensure that backup and data storage concepts exist for each relevant platform/component in its area of responsibility. Backups, retention periods and recovery tests are implemented. The backup concepts and recovery procedures are suitable for guaranteeing the agreed availability levels.	Der VERTRAGSPARTNER stellt sicher, dass für jede relevante Plattform/Komponente in seinem Verantwortungsbereich Sicherungs- und Datenhaltungskonzepte existieren. Backups, Aufbewahrungsfristen und Wiederherstellungstests werden umgesetzt. Die Sicherungskonzepte und Wiederherstellungs-verfahren sind geeignet, die vereinbarten Verfügbarkeitsstufen zu gewährleisten.

5 Überwachung, Prüfung und Berichterstattung / Monitoring, Audit, Reporting:

5.1 SECURITYAUDIT, MONITORING AND REPORTING SICHERHEITSPRÜFUNG, ÜBERWACHUNG UND REPORTING

The CONTRACTUAL PARTNER has appropriate security measures (in particular with regard to cyber threats) for data, applications and systems. The CONTRACTUAL PARTNER regularly evaluates the effectiveness of the security measures in relation to known cyber threats and cases of fraud as well as corresponding models (e.g. on the basis of current threat catalogues of the National Institute of Standards and Technology and the Federal Office for Information Security).	Der VERTRAGSPARTNER verfügt über angemessene Sicherheitsmaßnahmen (insbesondere im Hinblick auf Cyber-Bedrohungen) für Daten, Anwendungen und Systeme. Der VERTRAGSPARTNER evaluiert regelmäßig die Wirksamkeit der Sicherheitsmaßnahmen in Bezug auf bekannte Cyber-Bedrohungen und Betrugsfälle sowie entsprechende Modelle (z.B. auf der Grundlage aktueller Bedrohungskataloge des National Institute of Standards and Technology sowie des Bundesamts für Sicherheit in der Informationstechnik).
The CONTRACTUAL PARTNER shall plan and carry out vulnerability analyses and penetration tests at regular intervals for the systems and services provided for the CLIENT. Penetration tests for these systems must be carried out in the following manner: (1) at regular intervals based on the risk (2) Penetration tests shall be carried out by testers with sufficient knowledge, skills and experience who were not involved in the development of the security measures.	Der VERTRAGSPARTNER plant und führt in regelmäßigen Abständen Schwachstellenanalysen und Penetrationstests für Systeme und Dienste durch, die für den KUNDEN bereitgestellt werden. Penetrationstests für diese Systeme müssen in folgender Weise durchgeführt werden: (1) in regelmäßigen Abständen auf Grundlage des Risikos (2) Penetrationstests werden von Testern mit ausreichenden Kenntnissen, Fähigkeiten und Erfahrungen durchgeführt, die nicht an der Entwicklung der Sicherheitsmaßnahmen beteiligt waren.

The vulnerabilities identified and the results must be managed appropriately: Analysis, classification and remediation. Remedial actions must be carried out in a timely manner according to their criticality. The CONTRACTUAL PARTNER must provide summarized vulnerability assessment and/or penetration test results reports upon request.	Die aufgedeckten Schwachstellen und die Ergebnisse müssen in geeigneter Weise verwaltet werden: Analyse, Klassifizierung und Behebung. Die Abhilfemaßnahmen müssen entsprechend ihrer Kritikalität zeitnah durchgeführt werden. Der VERTRAGSPARTNER muss auf Anfrage zusammenfassende Ergebnisberichte von Schwachstellenbewertungen und/oder Penetrationstests zur Verfügung stellen.
The CONTRACTUAL PARTNER shall ensure that security problems reported by the CLIENT are rectified within a reasonable timeframe.	Der VERTRAGSPARTNER stellt sicher, dass vom KUNDEN gemeldete Sicherheitsprobleme innerhalb eines angemessenen Zeitrahmens behoben werden.
The CLIENT reserves the right to conduct security audits. The CLIENT shall notify the CONTRACTUAL PARTNER in advance and ensure that the audit is carried out during normal business hours and with minimal disruption to the CONTRACTUAL PARTNER's business. The CLIENT reserves the right to exercise its right to audit.	Der KUNDE behält sich das Recht vor, Sicherheitsaudits (bspw. Sicherheitsüberprüfung) durchzuführen. Der KUNDE benachrichtigt den VERTRAGSPARTNER im Voraus und stellt sicher, dass das Audit während der normalen Geschäftszeiten und mit minimaler Unterbrechung des Geschäftsbetriebs des VERTRAGSPARTNERS durchgeführt wird.

5.2 LOGGING & MONITORING

The CONTRACTUAL PARTNER has taken appropriate measures to ensure the traceability and retraceability of the operations carried out. The logs must contain sufficient information to determine the cause of a (security) problem and to enable the recovery of a series of events. The logs must be made available to the CLIENT if the CLIENT has legitimate reasons. The logs must record access attempts, information about system and network security events, warnings, failures and errors. The integrity of the log files must be guaranteed. Access to the log files must be restricted.	Der VERTRAGSPARTNER hat geeignete Maßnahmen ergriffen, um die Nachvollziehbarkeit und Rückverfolgbarkeit der durchgeführten Vorgänge zu gewährleisten. Die Protokolle müssen ausreichende Angaben enthalten, um die Ursache eines (Sicherheits-)Problems zu ermitteln und die Wiederherstellung einer Reihe von Ereignissen zu ermöglichen. Die Protokolle müssen dem KUNDEN zur Verfügung gestellt werden, wenn der KUNDE berechtigte Gründe hat. In den Protokollen müssen Zugriffsversuche, Informationen über System- und Netzsicherheitsereignisse, Warnungen, Ausfälle und Fehler aufgezeichnet werden. Die Integrität der Protokolldateien muss gewährleistet sein. Der Zugang zu den Protokolldateien muss eingeschränkt werden.

5.3 INCIDENT MANAGEMENT AND REPORTING

The CONTRACTUAL PARTNER shall have documented procedures for information security incidents that enable effective and proper handling of security incidents. The procedures shall include reporting, analyzing, monitoring, resolving and documenting security incidents.	Der VERTRAGSPARTNER muss über dokumentierte Verfahren für Informationssicherheitsvorfälle verfügen, die eine wirksame und ordnungsgemäße Handhabung von Sicherheitsvorfällen ermöglichen. Die Verfahren müssen die Meldung, Analyse, Überwachung, Lösung und Dokumentation von Sicherheitsvorfällen umfassen.
Security incidents by the CONTRACTUAL PARTNER that are related to data or services for the CLIENT or may have a direct impact on the CLIENT must be reported to the CLIENT within 48 hours of becoming aware of them, in the case of critical incidents immediately. The	Sicherheitsvorfälle beim VERTRAGSPARTNER, die im Zusammenhang mit Daten oder Dienstleistungen für den KUNDEN stehen oder unmittelbare Auswirkungen auf diesen haben können, müssen innerhalb von 48 Stunden nach Bekanntwerden, bei kritischen Vorfällen unmittelbar, an den KUNDEN gemeldet werden.

CONTRACTUAL PARTNER shall continuously provide all relevant information to assist the CLIENT in dealing with the incident. A security incident report must be sent to the address security-alert@witt-gruppe.eu. The report must indicate what type of security incident it is and how the criticality is assessed. In addition, the notification shall contain all available information pertinent to the incident, including the data concerned, the contact person at the CONTRACTUAL PARTNER and the standard contact person at the CLIENT, and shall be continuously updated.	Er stellt kontinuierlich alle relevanten Informationen bereit, um den KUNDEN bei der Bewältigung des Vorfalls zu unterstützen. Eine Sicherheitsvorfallmeldung muss an die Adresse security-alert@witt-gruppe.eu erfolgen. Aus der Meldung muss hervorgehen um was für eine Art von Sicherheitsvorfall es sich handelt und wie die Kritikalität bewertet wird. Ferner enthält die Meldung sämtliche verfügbaren Informationen zum Vorfall, einschließlich der betroffenen Daten, der Kontaktperson beim VERTRAGSPARTNER sowie des standardmäßigen Ansprechpartners beim KUNDEN und wird kontinuierlich auf den neuesten Stand gebracht.
The CONTRACTUAL PARTNER shall support the CLIENT in fulfilling any reporting and documentation obligations regarding a security incident, in particular vis-à-vis responsible authorities, as well as in eliminating the effects of security incidents and minimizing the damage, free of charge.	Der VERTRAGSPARTNER wird den KUNDEN bei der Erfüllung etwaiger Melde- und Dokumentationspflichten bezüglich eines Sicherheitsvorfalls, insbesondere gegenüber von zuständigen Behörden, sowie bei der Beseitigung der Auswirkungen von Sicherheitsvorfälle und der Minimierung der Schäden vollumfänglich kostenlos unterstützen.