Security Requirements for Suppliers (SRS) / Sicherheitanforderungen für Lieferanten

of / der

Raiffeisen Informatik GmbH & Co KG
Lilienbrunngasse 7-9, 1020 Wien

(subsequently called “CUSTOMER” / nachfolgend „KUNDE“ genannt)

effective from December, 1st 2021 / gültig ab 01.Dezember 2021

Delivering trusted services is an integral part of our corporate strategy. Using innovative services and products as well as cooperating with professional partners and suppliers, meeting our security requirements is necessary to stay ahead in a fast-changing industry.

Die Erbringung vertrauenswürdiger Dienstleistungen ist ein integraler Bestandteil unserer Unternehmensstrategie. Der Einsatz innovativer Dienstleistungen und Produkte sowie die Zusammenarbeit mit professionellen und unsere Sicherheitsanforderungen erfüllenden Partnern und Lieferanten ist dabei notwendig, um in einer sich schnell verändernden Branche erfolgreich zu sein.

It is our due diligence to protect our as well as our client’s data, systems and applications with security measures according to leading industry standards as it is expected from an IT-provider, serving international financial institution.
Managing supplier relationships in regard to security is an important part of internal risk management framework, a common praxis (e.g. ISO 27000 series, NIST Cybersecurity Framework) and mandatory for financial institutions (e.g. the EBA Guidelines on ICT and security risk management dated 29 November 2019, § 25 and the Annex to § 25 of the Austrian Banking Act, etc.), together further referred to as the "Security Requirements".

Es gehört zu unserer Sorgfaltspflicht, sowohl unsere als auch die Daten, Systeme und Anwendungen unserer Kunden mit Sicherheitsmaßnahmen nach führenden Industriestandards zu schützen, wie es von einem IT-Provider internationaler Finanzinstitute erwarten wird.
Das Management von Lieferantenbeziehungen in Bezug auf die Sicherheit ist ein wichtiger Teil des internen Risikomanagements, eine gängige Praxis (zB. ISO 27000-Serie, NIST Cybersecurity Framework) und für Finanzinstitute verpflichtend (zB. die EBA-Leitlinien zum IKT- und Sicherheitsrisikomanagement vom 29. November 2019, § 25 und der Anhang zu § 25 des österreichischen Bankwesengesetzes usw.), die im Folgenden als "Sicherheitsanforderungen" bezeichnet werden.

The Security Requirements are derived from established industry standards and based on best practices, which can be expected from a service provider in the financial sector.

Die Sicherheitsanforderungen leiten sich von etablierten Branchenstandards ab und basieren auf Best Practices, die von einem Dienstleister im Finanzsektor erwartet werden können.

Having regard to the above, the Vendor, Processor or Partner (collectively referred to as “SUPPLIER”) represents and warrants that it has made all necessary due diligence and is familiar with and acknowledges the Security Requirements and agrees to comply with the Security Requirements in general, as well when (a) accessing CUSTOMER facilities, Networks and/or Information Systems, or (b) accessing, processing, or storing CUSTOMER information/data, or (c) providing infrastructure services and/or standard software, developing software.
Whenever these SRS or any other requirements talk

In Anbetracht des Vorstehenden sichert der Anbieter, Auftragsverarbeiter oder Partner (gemeinsam als „LIEFERANT" bezeichnet) zu und gewährleistet, dass er alle erforderlichen Sorgfaltspflichten erfüllt hat und mit den Sicherheitsanforderungen vertraut ist und diese anerkennt und sich verpflichtet, die Sicherheitsanforderungen im Allgemeinen einzuhalten, wenn er (a) auf Einrichtungen, Netze und/oder Informationssysteme des KUNDEN zugreift oder (b) auf Informationen/Daten des KUNDEN zugreift, diese verarbeitet oder speichert oder (c) Infrastrukturdienste und/oder Standardsoftware bereitstellt oder Software entwickelt.

Whenever the term "CUSTOMER" is used in this Security Policy, it shall mean not only the respective data (or systems, services, etc.) of R-IT, but also those of its customers.

Additional security requirements may be specified in individual agreements (e.g. SLA, statement of work).

The German version is for information purpose only. The English version shall prevail.

Wann immer in diesen Sicherheitsrichtlinie von "KUNDE" die Rede ist, sind sinngemäß nicht nur die jeweiligen Daten (bzw. Systeme, Services, etc.) der R-IT, sondern auch die ihrer Kunden zu verstehen.

Zusätzliche Sicherheitsanforderungen können in Einzelvereinbarungen (zB. SLA, statement of work) festgelegt werden.

Die deutsche Version dient nur zur Information. Die englische Fassung ist maßgebend.

ICT Governance	ICT Governance
Guidelines	**Richtlinien**
The SUPPLIER maintains an information security management system including a continuous improvement process based on recognized industry standards.	Der LIEFERANT unterhält ein Managementsystem für die Informationssicherheit, das einen kontinuierlichen Verbesserungsprozess auf der Grundlage anerkannter Branchenstandards umfasst.
Information security policies, procedures, roles, responsibilities and accountabilities are defined in accordance with SUPPLIER`s business requirements, relevant laws and regulations. Information security policies are approved by management, published and communicated to employees and relevant external parties.	Informationssicherheitsrichtlinien, -verfahren, -rollen, -verantwortlichkeiten und -zuständigkeiten werden in Übereinstimmung mit den Geschäftsanforderungen des LIEFERANTEN und den einschlägigen Gesetzen und Vorschriften festgelegt. Die Informationssicherheitsrichtlinien werden von der Geschäftsleitung genehmigt, veröffentlicht und an die Mitarbeiter und relevanten externen Parteien weitergegeben.
The SUPPLIER regularly reviews its compliance to established security policies, standards and any other security requirements.	Der LIEFERANT überprüft regelmäßig, ob er die festgelegten Sicherheitsrichtlinien und -standards sowie alle anderen Sicherheitsanforderungen einhält.
Risk Management	**Risikomanagement**
The SUPPLIER has a security risk management in place. The SUPPLIER ensures that risks, which directly or indirectly affect CUSTOMER services and/or data, are assessed and mitigation measures are in place and documented. Risks which directly or indirectly affect the CUSTOMER must be reported on demand.	Der LIEFERANT verfügt über ein Sicherheitsrisikomanagement. Der LIEFERANT stellt sicher, dass Risiken, die sich direkt oder indirekt auf die Dienste und/oder Daten des KUNDEN auswirken, bewertet und Maßnahmen zur Risikominderung ergriffen und dokumentiert werden. Risiken, die den KUNDEN direkt oder indirekt betreffen, müssen auf Verlangen gemeldet werden.
Contractual Agreement	**Vertragliche Vereinbarung**
The SUPPLIER must include responsibilities for information security in contractual agreements with their employees and contractors.	Der LIEFERANT muss die Verantwortung für die Informationssicherheit in die vertraglichen Vereinbarungen mit seinen Mitarbeitern und Auftragnehmern aufnehmen.
Background Checks	**Hintergrund-Checks**
Background verification checks on candidates for employment are carried out in accordance with relevant laws and regulations. The level of verification performed must be proportional to the risk associated with the candidate's role.	Die Überprüfung des Hintergrunds von Bewerbern für eine Beschäftigung erfolgt in Übereinstimmung mit den einschlägigen Gesetzen und Vorschriften. Der Umfang der Überprüfung muss im Verhältnis zu dem mit der Funktion des Bewerbers verbundenen Risiko stehen.
Awareness Program	**Sensibilisierungsprogramm**
All employees of the SUPPLIER and, where relevant, contractors receive awareness education and trainings appropriate for their job function. Additionally, updates of SUPPLIER`s policies and procedures are communicated to employees as well. All personnel must have adequate skills related to their roles and responsibilities.	Alle Mitarbeiter des LIEFERANTEN und gegebenenfalls auch die Auftragnehmer erhalten eine ihrer Funktion entsprechende Sensibilisierung und Schulung. Darüber hinaus werden die Mitarbeiter auch über Aktualisierungen der Richtlinien und Verfahren des LIEFERANTEN unterrichtet. Das gesamte Personal muss über die für seine Aufgaben und Zuständigkeiten erforderlichen Kenntnisse verfügen.
ICT Project and Change management	**ICT Projekt- und Changemanagement**
Asset Lifecycle	**Asset-Lebenszyklus**
The SUPPLIER ensures that information security is an integral part of information systems across their entire lifecycle (acquisition to decommission of assets).	Der LIEFERANT stellt sicher, dass die Informationssicherheit ein integraler Bestandteil der Informationssysteme über deren gesamten Lebenszyklus ist (Erwerb bis Stilllegung der Anlagen).

The SUPPLIER ensures that provided software is supported by operating systems and middleware (e.g. Java) versions, which receive security updates and are not end-of-life. The SUPPLIER provides regular, in time security updates over the entire contract lifecycle.	Der LIEFERANT stellt sicher, dass die bereitgestellte Software von Betriebssystemen und Middleware (zB. Java) unterstützt wird, die Sicherheitsupdates erhalten und nicht veraltet sind. Der LIEFERANT sorgt für regelmäßige, rechtzeitige Sicherheitsupdates während des gesamten Vertragslebenszyklus.
Software Change Management	**Software Change Management**
The SUPPLIER has formal change management and secure software development lifecycle policies that also define security related controls. Cybersecurity reviews for new system designs or changes to systems, and security testing prior to deployment must be part of the processes. Changes are appropriately requested, authorized, tested and approved prior release to production.	Der LIEFERANT verfügt über formale Richtlinien für das Change Management und den Lebenszyklus der sicheren Softwareentwicklung, die auch sicherheitsrelevante Kontrollen festlegen. Überprüfungen der Cybersicherheit bei neuen Systemdesigns oder Änderungen an Systemen sowie Sicherheitstests vor der Bereitstellung müssen Teil der Prozesse sein. Änderungen werden in angemessener Weise angefordert, autorisiert, getestet und genehmigt, bevor sie für die Produktion freigegeben werden.
Secure Software Development Lifecycle	**Lebenszyklus der sicheren Softwareentwicklung**
The SUPPLIER includes information security aspects in the product documentation. This documentation must contain instructions for the configuration of the service and/or the environment in order to ensure a secure operation. Developed software must be tested in a controlled environment in order to detect weaknesses before it is provided to the CUSTOMER.	Der LIEFERANT 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 dem KUNDEN zur Verfügung gestellt wird.
The SUPPLIER ensures that the software development lifecycle contains appropriate security measures (Secure Software Development Lifecycle). This includes but is not limited to: -Usage of internationally recognized secure software development methods (including agile processes such as Scrum, Kanban, etc.) as integral part of the secure software development process -Secure coding guidelines based on international standards -Integrity of source code is ensured -Periodically carry out secure code reviews (Static Application Security Testing and Dynamic Application Security Testing) -Vulnerability scanning which also includes used third-party code and open source components (e.g. libraries) -Penetration tests which are performed by an independent third party -Appropriate trainings for internal and external software developers Findings and known vulnerabilities are mitigated before release to production.	Der LIEFERANT stellt sicher, dass der Lebenszyklus der Softwareentwicklung angemessene Sicherheitsmaßnahmen enthält (Secure Software Development Lifecycle). Dies beinhaltet, ist aber nicht beschränkt auf: -Einsatz international anerkannter, sicherer Softwareentwicklungsmethoden (einschließlich agiler Prozesse wie Scrum, Kanban, etc.) als integraler Bestandteil des sicheren Softwareentwicklungsprozesses -Sichere Coding-Richtlinien auf der Grundlage internationaler Normen -Die Integrität des Quellcodes ist gewährleistet. -Regelmäßige Überprüfung des sicheren Codes (statische und dynamische Anwendungs-sicherheitstests) -Schwachstellen-Scans, die auch den verwendet-en Code von Drittanbietern und Open-Source-Komponenten (zB. Bibliotheken) umfassen -Penetrationstests, die von einer unabhängigen dritten Partei durchgeführt werden -Angemessene Schulungen für interne und externe Softwareentwickler Gefundene und bekannte Schwachstellen werden vor der Freigabe für die Produktion beseitigt.

Outsourcing	Outsourcing
Sub-Outsourcing	**Sub-Outsourcing**
The SUPPLIER has clear contractual agreements with any SUB-SUPPLIERs of services, in order to state their responsibility for the security of CUSTOMER data they process / store / transmit on behalf of the CUSTOMER. The SUPPLIER ensures that security measures implemented by the SUB-SUPPLIERs have at least the same level as stated within this document and prime contract. The SUPPLIER verifies the effectiveness of the measures as part of their supplier management process.	Der LIEFERANT hat klare vertragliche Vereinbarungen mit allen Unterauftragnehmern von Dienstleistungen, um deren Verantwortung für die Sicherheit der KUNDENDATEN, die sie im Auftrag des KUNDEN verarbeiten / speichern / übermitteln, festzulegen. Der LIEFERANT stellt sicher, dass die von den UNTERAUFTRAGNEHMERN eingeführten Sicherheitsmaßnahmen mindestens das in diesem Dokument und im Hauptvertrag angegebene Niveau haben. Der LIEFERANT prüft die Wirksamkeit der Maßnahmen im Rahmen seines Lieferantenmanagementprozess.
Information Security	**Informationssicherheit**
Identity and Access Management	**Identitäts- und Zugriffsmanagement**
The SUPPLIER has access controls in place in order to verify identities and restrict access to authorized users only. Access rights are based on "need to know" and "least privilege" principles. Additionally, the principle of "separation of duties" is adhered to.	Der LIEFERANT hat Zugangskontrollen eingerichtet, um Identitäten zu überprüfen und den Zugang auf autorisierte Benutzer zu beschränken. Die Zugriffsrechte beruhen auf den Grundsätzen "Kenntnisnahme erforderlich" und "geringstmögliches Privileg". Darüber hinaus wird der Grundsatz der "Aufgabentrennung" beachtet.
The SUPPLIER has implemented authentication mechanisms to protect accesses to systems, according to best practices which include but are not limited to:- password policies (minimum lengths, complexity, avoiding re-use) -unique user identification (generic and shared users are avoided) -secure storage / management / transmission of credentials	Der LIEFERANT hat Authentifizierungs-mechanismen 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
SUPPLIER ensures that accounts which are used for access over the internet are protected by strong authentication mechanisms (e.g. multi-factor authentication).	Der LIEFERANT stellt sicher, dass Konten, die für den Zugang über das Internet genutzt werden, durch starke Authentifizierungsmechanismen (zB. Multi-Faktor-Authentifizierung) geschützt sind.
The SUPPLIER has implemented strong controls for privileged accounts (e.g. system administrators) by means of strong authentication, limitation to a minimum and closely supervised usage (e.g. multi-factor authentication).	Der LIEFERANT hat strenge Kontrollen für privilegierte Konten (zB. Systemadministratoren) durch starke Authentifizierung, Beschränkung auf ein Minimum und streng überwachte Nutzung (zB. Multi-Faktor-Authentifizierung) eingeführt.
The SUPPLIER shall review the access rights of its staff on regular intervals and shall change (i.e. restrict or revoke) the access rights if necessary.	Der LIEFERANT überprüft die Zugriffsrechte seiner Mitarbeiter in regelmäßigen Abständen und ändert (d.h. beschränkt/widerruft) sie, falls erforderlich.
Patch Management	**Patch Management**
The SUPPLIER periodically analyzes systems (operating systems, applications, network components) for known vulnerabilities. Patches are applied in a consistent, standardized manner and prioritized based on criticality. If the root cause of vulnerabilities could not be mitigated within reasonable time, alternative risk mitigation measures must be implemented until the root cause is remedied. The SUPPLIER has implemented an emergency change process.	Der LIEFERANT analysiert regelmäßig die Systeme (Betriebssysteme, Anwendungen, Netzkomponenten) auf bekannte Schwachstellen. Patches werden in einer konsistenten, standardisierten Weise angewendet und nach ihrer Kritikalität priorisiert. Wenn die Ursache von Schwachstellen nicht innerhalb eines angemessenen Zeitraums beseitigt werden kann, müssen bis zur Behebung alternative Maßnahmen zur Risikominderung ergriffen werden. Der LIEFERANT hat einen Notfall-Changeprozess implementiert.

Network Security	Netzwerksicherheit
The SUPPLIER has implemented and maintained network security infrastructure components such as firewalls, intrusion detection/prevention systems (IDS/IPS) and other security controls, providing detection, continuous monitoring, and restrictive network traffic flow to assist in limiting the impact of attacks. Systems with a higher risk level (e.g. externally exposed) must have stricter measures in place.	Der LIEFERANT hat Komponenten der Netzsicherheitsinfrastruktur wie Firewalls, Intrusion Detection/Prevention Systeme (IDS/IPS) und andere Sicherheitskontrollen 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 (zB. für einen Zugriff von externen Netzwerken erreichbar) müssen strengere Maßnahmen ergriffen werden.
The SUPPLIER ensures that a formal remote access policy is in place.	Der LIEFERANT stellt sicher, dass eine formelle Fernzugriffsrichtlinie vorhanden ist.
The SUPPLIER ensures segregation and segmentation of the environments according to industry standards, when: (1) environments are shared with other customers; and/or (2) SUPPLIER implements test, quality and production environments.	Der LIEFERANT stellt die Trennung und Segmentierung der Umgebungen gemäß den Industriestandards sicher, wenn: (1) Umgebungen gemeinsam mit anderen Kunden genutzt werden; und/oder (2) der LIEFERANT Test-, Qualitäts- und Produktionsumgebungen einrichtet.
Encryption	**Verschlüsselung**
The SUPPLIER ensures an appropriate level of protection of data confidentiality. The SUPPLIER must also consider specific measures for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture. The encryption is compliant to leading standards and guidelines or equivalent (e.g. National Institute of Standards and Technology - NIST).	Der LIEFERANT gewährleistet einen angemessenen Schutz der Vertraulichkeit der Daten. Der LIEFERANT muss auch spezifische Maßnahmen für Daten bei der Übertragung sowie in flüchtigen und persistenten Speicher 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 (zB. National Institute of Standards and Technology - NIST).
The SUPPLIER protects mobile devices and external electronic media (e.g. USB memory storage, tape) against unauthorized access, through adequate physical and logical security measures. Data-at-rest encryption on these devices must be enforced.	Der LIEFERANT schützt mobile Geräte und externe elektronische Medien (zB. USB-Speicher, Band) durch angemessene physische und logische Sicherheitsmaßnahmen vor unbefugtem Zugriff. Die Verschlüsselung von auf diesen Geräten gespeicherten Daten muss durchgesetzt werden.
Malware Protection	**Schutz vor Schadsoftware**
The SUPPLIER protects servers and endpoints with proper Malware protection which is kept up to date. The software must detect if anti-virus/malware software on devices has been disabled or not receiving regular updates.	Der LIEFERANT schützt die Server und Endgeräte mit einem angemessenen Schutz vor Malware, der stets auf dem neuesten Stand gehalten wird. Die Software muss erkennen, ob die Antiviren-/Malware-Software auf den Geräten deaktiviert wurde oder nicht regelmäßig aktualisiert wird.
Security Testing, Monitoring & Reporting	**Sicherheitsprüfung, Überwachung und Reporting**
The SUPPLIER has appropriate security measures (in particular related to cyber threats) for data, applications and systems. The SUPPLIER periodically evaluates the effectiveness of security measures related to known cyber threats and frauds as well as respective models (e.g. based on up-to-date threat catalogues like National Institute of Standards and Technology, Bundesamt für Sicherheit in der Informationstechnik).	Der LIEFERANT verfügt über angemessene Sicherheitsmaßnahmen (insbesondere im Hinblick auf Cyber-Bedrohungen) für Daten, Anwendungen und Systeme. Der LIEFERANT evaluiert regelmäßig die Wirksamkeit der Sicherheitsmaßnahmen in Bezug auf bekannte Cyber-Bedrohungen und Betrugsfälle sowie entsprechende Modelle (zB. auf der Grundlage aktueller Bedrohungskataloge wie National Institute of Standards and Technology, Bundesamt für Sicherheit in der Informationstechnik).

The SUPPLIER has periodic plans and executes Vulnerability Assessments and Penetration Tests on systems used to provide service to the CUSTOMER. Penetration Tests on these systems have to be conducted in the following manner: (1) at least once a year (2) in case of a major release/updates of applications/software/information services (3) Penetration tests are carried out by testers with sufficient knowledge, skills and expertise and who were not involved in the development of the security measures. The discovered vulnerabilities and the findings must be managed appropriately: Analysis, classification and remediation. Mitigation actions must be performed according to their criticality in a timely manner. The SUPPLIER must provide summary result reports of Vulnerability Assessments and/or Penetration Tests on demand.	Der LIEFERANT plant und führt in regelmäßigen Abständen Schwachstellenanalysen und Penetrationstests für die Systeme durch, die zur Erbringung der Dienstleistung für den KUNDEN eingesetzt werden. Penetrationstests für diese Systeme müssen in folgender Weise durchgeführt werden: (1) mindestens einmal pro Jahr (2) im Falle einer größeren Release/Aktualisierung von Anwendungen/Software/Informations-diensten (3) Penetrationstests werden von Testern mit ausreichenden Kenntnissen, Fähigkeiten und Erfahrungen durchgeführt, die nicht an der Entwicklung der Sicherheitsmaßnahmen beteiligt waren. 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 LIEFERANT muss auf Anfrage zusammenfassende Ergebnisberichte von Schwachstellenbewertungen und/oder Penetrationstests zur Verfügung stellen.
The SUPPLIER ensures that security issues identified and reported by the CUSTOMER are resolved within a reasonable timeframe.	Der LIEFERANT stellt sicher, dass vom KUNDEN gemeldete Sicherheitsprobleme innerhalb eines angemessenen Zeitrahmens behoben werden.
The CUSTOMER reserves the right to perform security assessments to verify compliance with here listed requirements. The CUSTOMER notifies the SUPPLIER in advance and ensures the audit is performed during normal business hours, and with minimal disruption to the SUPPLIER's business operations. Upon request, the SUPPLIER must confirm, in writing, the SUPPLIER's compliance with the requirements of here listed requirements and provide written responses to any questions that the CUSTOMER presents to the SUPPLIER regarding its security practices.	Der KUNDE behält sich das Recht vor, Sicherheitsbewertungen durchzuführen, um die Einhaltung der hier aufgeführten Anforderungen zu überprüfen. Der KUNDE benachrichtigt den LIEFERANTEN im Voraus und stellt sicher, dass das Audit während der normalen Geschäftszeiten und mit minimaler Unterbrechung des Geschäftsbetriebs des LIEFERANTEN durchgeführt wird. Auf Anfrage muss der LIEFERANT die Einhaltung der hier aufgeführten Anforderungen schriftlich bestätigen und alle Fragen des KUNDEN an den LIEFERANTEN zu seinen Sicherheitsverfahren schriftlich beantworten.
System Hardening	**System Hardening**
The SUPPLIER has configured and deployed their ICT assets (e.g. databases, applications, operating systems, network devices) using a secure baseline (hardening). The secure baseline is based on best practices (e.g. CIS standards) or equivalent. The hardening configurations on the ICT assets are periodically reviewed and updated.	Der LIEFERANT hat seine IT-Ressourcen (zB. Datenbanken, Anwendungen, Betriebssysteme, Netzwerkgeräte) unter Verwendung einer sicheren Grundlage (Hardening) konfiguriert und eingesetzt. Die Sicherheitsgrundlagen basieren auf Best Practices (zB. CIS-Standards) oder gleichwertigen Verfahren. Die Konfigurationen für die IT-Anlagen werden regelmäßig überprüft und aktualisiert.

ICT Operations	ICT Betrieb
Data Management	**Data Management**
The SUPPLIER ensures that measures against data loss and leakage are in place.	Der LIEFERANT stellt sicher, dass Maßnahmen gegen Datenverlust und -abfluss getroffen werden.
The SUPPLIER must not replicate CUSTOMER production data or use it in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from the CUSTOMER.	Der LIEFERANT 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.
Backup & Recovery	**Backup & Recovery**
The SUPPLIER ensures that backup and data retention concepts exist for each relevant platform/component under the responsibility of the SUPPLIER. Backups, retention periods and recovery tests are performed. Backup concepts and recovery procedures are suitable to ensure agreed availability levels.	Der LIEFERANT stellt sicher, dass für jede relevante Plattform/Komponente im Verantwortungsbereich des LIEFERANTEN Sicherungs- und Datenhaltungskonzepte existieren. Backups, Aufbewahrungsfristen und Wiederherstellungstests durchgeführt werden. Die Sicherungskonzepte und Wiederherstellungs-verfahren sind geeignet, die vereinbarten Verfügbarkeitsstufen zu gewährleisten.
Logging & monitoring	**Logging & Monitoring**
The SUPPLIER has adopted appropriate measures in order to ensure accountability and traceability of operations carried out. Logs must provide sufficient details to assist in the identification of the source of an (security) issue and enable a series of events to be recreated. Logs must be provided to the CUSTOMER if the CUSTOMER has justified reasons. Logs must record access attempts, system and network security event information, alerts, failures and errors. Integrity of log files must be ensured. Access to log files must be restricted.	Der LIEFERANT 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 Netzsicherheits-ereignisse, Warnungen, Ausfälle und Fehler aufgezeichnet werden. Die Integrität der Protokolldateien muss gewährleistet sein. Der Zugang zu den Protokolldateien muss eingeschränkt werden.
Incident Management & Reporting	**Incident Management & Reporting**
The SUPPLIER must have documented information Security Incident procedures, enabling effective and orderly management of Security Incidents. The procedures must cover the reporting, analysis, monitoring, resolution and documentation of Security Incidents.	Der LIEFERANT 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.
SUPPLIER notifies CUSTOMER without undue delay after becoming aware of an Incident which is directly or indirectly in connection with CUSTOMER related Services and Data and provide reasonable information in its possession to assist CUSTOMER to meet CUSTOMER'S obligations. SUPPLIER provides such information in phases as it becomes available. After verification of a security incident in connection with CUSTOMER related Services or Data, the SUPPLIER shall: i. provide written notification to the CUSTOMER´s Business Units and additionally to contacts defined in the contract and in time-critical cases or imminent danger also call R-IT's Help-Desk without undue delay.	Der LIEFERANT benachrichtigt den KUNDEN unverzüglich nach Bekanntwerden eines Vorfalls, der direkt oder indirekt mit den Diensten und Daten des KUNDEN zusammenhängt, und stellt alle ihm zur Verfügung stehenden Informationen zur Verfügung, um den KUNDEN bei der Erfüllung seiner Verpflichtungen zu unterstützen. Der LIEFERANT stellt diese Informationen schrittweise zur Verfügung, sobald sie verfügbar werden. Nach der Überprüfung eines Sicherheitsvorfalls in Verbindung mit den Diensten oder Daten des KUNDEN wird der LIEFERANT: i. die Geschäftsbereiche des KUNDEN und zusätzlich die im Vertrag definierten Kontakte schriftlich

ii. the notification shall include at least following details, if initially not all information is available, the SUPPLIER should provide details or imminent danger as soon as they are known in a staged reporting: • Contact information of SUPPLIER incident responsible • What occurred • How occurred • Why occurred • Components / assets affected • CUSTOMER services / data affected • Date and time the incident occurred • Date and time the incident was discovered • Business impact / effect for CUSTOMER services / data • Incident resolution • Action taken to resolve incident • Action planned to resolve incident iii. use all reasonable efforts to avoid and detect such incidents; iv. continuously inform the CUSTOMER of the measures the SUPPLIER is taking or intends to take; v. obtain the CUSTOMER´s prior written approval pursuant to Applicable Law in connection with any notification or public information with respect to such breach, and vi. coordinate any further activities with the CUSTOMER. vii. this reporting obligation also applies to sub-contractors	benachrichtigen und in zeitkritischen Fällen oder bei Gefahr im Verzug auch den Help-Desk von R-IT unverzüglich anrufen. ii. Die Meldung hat mindestens folgende Angaben zu enthalten, wenn zunächst nicht alle Informationen vorliegen, sollte der LIEFERANT die Angaben bei zeitkritischen Fällen oder Gefahr im Verzug sofort nach Bekanntwerden in einer gestaffelten Meldung nachliefern: - Kontaktinformationen der Person beim LIEFERANTEN, die für den Vorfall verantwortlich ist - Was ist passiert? - Wie ist es passiert - Warum ist es geschehen? - Betroffene Komponenten/Anlagen - Betroffene Dienste/Daten des KUNDEN - Datum und Uhrzeit des Auftretens des Vorfalls - Datum und Uhrzeit der Entdeckung des Vorfalls - Auswirkung auf das Geschäft / Auswirkungen auf KUNDEN-Services/ -Daten - Lösung des Vorfalls - Ergriffene Maßnahmen zur Behebung des Vorfalls - Geplante Maßnahmen zur Behebung des Vorfalls iii. alle angemessenen Anstrengungen zu unternehmen, um solche Vorfälle zu vermeiden und zu entdecken; iv. den KUNDEN laufend über die Maßnahmen zu informieren, die der LIEFERANT ergreift oder zu ergreifen beabsichtigt; v. die vorherige schriftliche Zustimmung des KUNDEN gemäß dem anwendbaren Recht in Verbindung mit jeglicher Benachrichtigung oder öffentlichen Information in Bezug auf eine solche Verletzung einzuholen, und vi. alle weiteren Aktivitäten mit dem KUNDEN zu koordinieren. vii. diese Meldepflicht gilt auch für Subauftragnehmer
Physical Security	**Physische Sicherheit**
Physical Access	**Physischer Zugang**
The SUPPLIER has categorized its premises into different protection zones, reflecting certain security measures and access rights according to the relevant security needs.	Der LIEFERANT hat seine Räumlichkeiten in verschiedene Schutzzonen eingeteilt, die bestimmte Sicherheitsmaßnahmen und Zugangsrechte entsprechend den jeweiligen Sicherheitsanforderungen widerspiegeln.
Access to IT systems such as servers is further restricted with special protection zones for authorized personnel only.	Der Zugang zu IT-Systemen wie zB. Servern ist durch spezielle Schutzzonen, die nur für befugtes Personal zugänglich sind, weiter eingeschränkt.
Only secure data center facilities must be used to store CUSTOMER data.	Für die Speicherung von Daten des KUNDEN dürfen nur sichere Rechenzentren verwendet werden

Business Continuity Management	Business Continuity Management
BCM	**BCM**
The SUPPLIER has up to date and maintained Disaster Recovery Plans and Business Continuity Plans in place. The Disaster Recovery Plans and Business Continuity Plans must be designed to prevent negativ impacts by unplanned disruptions to maximum possible extend and to ensure, that the SUPPLIER can continue to function through operational interruption and continue to provide Services as specified in its agreement with the CUSTOMER. The SUPPLIER will provide the CUSTOMER written summaries of its Disaster Recovery Plans and Business Continuity Plans upon request.	LIEFERANT verfügt über aktuelle und aufrechterhaltene Notfallpläne und Pläne zur Aufrechterhaltung des Geschäftsbetriebs. Die Disaster-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 LIEFERANT auch bei Betriebsunterbrechungen weiterarbeiten und die Dienstleistungen gemäß dem Vertrag mit dem KUNDEN erbringen kann. Der LIEFERANT stellt dem KUNDEN auf Anfrage schriftliche Zusammenfassungen seiner Disaster-Recovery-Pläne und Business-Continuity-Pläne zur Verfügung.
The SUPPLIER performs at least annual, adequate tests of their own Business Continuity Plans and Disaster Recovery Plans. Service relevant test results must be provided to the CUSTOMER on demand or at least if the tests have been carried out.	LIEFERANT führt mindestens einmal jährlich angemessene Tests seiner eigenen Business-Continuity- und Disaster-Recovery-Pläne durch. Servicerelevante Testergebnisse sind dem KUNDEN auf Verlangen, zumindest aber nach Durchführung der Tests zur Verfügung zu stellen.
The SUPPLIER has ensured the scope of the Business Continuity Plans and Disaster Recovery Plans encompasses all locations, personnel and information systems used to perform or provide services for the CUSTOMER.	LIEFERANT hat sichergestellt, dass der Geltungsbereich der Business Continuity- und Notfallwiederherstellungspläne alle Standorte, Mitarbeiter und Informationssysteme umfasst, die zur Erbringung von Dienstleistungen für den KUNDEN eingesetzt werden.