Security Requirements for Suppliers (SRS)

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 fastchanging industry.

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".

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.

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
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 SK, but also those of its customers.
Additional security requirements may be specified in individual agreements (e.g. SLA, statement of work).

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

Bezpečnostné požiadavky pre dodávateľov (SRS)

Poskytovanie dôveryhodných služieb je neoddeliteľnou súčasťou našej firemnej stratégie. Využívanie inovatívnych služieb a produktov a spolupráca s profesionálnymi partnermi a dodávateľmi, ktorí spĺňajú naše bezpečnostné požiadavky, sú nevyhnutné na dosiahnutie úspechu v rýchlo sa meniacom odvetví.

Našou povinnosťou je chrániť naše údaje, systémy a aplikácie, ako aj údaje našich zákazníkov, bezpečnostnými opatreniami v súlade s poprednými priemyselnými štandardmi, ako sa to očakáva od poskytovateľa IT pre medzinárodné finančné inštitúcie.
Riadenie vzťahov s dodávateľmi z hľadiska bezpečnosti je dôležitou súčasťou interného riadenia rizík, bežnou praxou (napr. ISO 27000, NIST Cybersecurity Framework) a povinnou pre finančné inštitúcie (napr. usmernenia EBA o ICT a riadení bezpečnostných rizík z 29. novembra 2019, paragraf 25 a príloha k paragrafu 25 rakúskeho zákona o bankách atď.), spoločne ďalej označované ako "bezpečnostné požiadavky".

Bezpečnostné požiadavky sú odvodené od zavedených priemyselných noriem a vychádzajú z osvedčených postupov, ktoré možno očakávať od poskytovateľa služieb vo finančnom sektore.

Vzhľadom na vyššie uvedené, Poskytovateľ, Spracovateľ alebo Partner (ďalej spoločne len "DODÁVATEĽ") vyhlasuje a zaručuje, že vykonal všetky potrebné opatrenia, je oboznámený s bezpečnostnými požiadavkami a berie ich na vedomie a zaväzuje sa dodržiavať bezpečnostné požiadavky vo všeobecnosti pri (a) prístupe k zariadeniam, sieťam a/alebo informačným systémom ZÁKÁZNÍKA alebo (b) prístupe, spracovávní, uchovávaní informácii/ údajov, c) alebo pri poskytovaní služby infraštruktúry a/alebo dodaní štandardného softvéru, vývoji softvéru.

Kedykoľvek, keď v týchto SRS alebo akýchkoľvek iných požiadavkách je uvedený pojem "ZÁKAZNÍK", znamená to nielen príslušné údaje (alebo systémy, služby atď.) spoločnosti R-IT SK, ale aj údaje jej zákazníkov.
Ďalšie bezpečnostné požiadavky môžu byť špecifikované v jednotlivých dohodách (napr. SLA, výkaz práce).
Slovenská verzia má len informatívny charakter.
Rozhodujúca je anglická verzia.

ICT Governance	ICT Governance
Guidelines	**Usmernenia**
The SUPPLIER maintains an information security management system including a continuous improvement process based on recognized industry standards.	DODÁVATEĽ musí udržiavať systém riadenia bezpečnosti informácií, ktorý zahŕňa proces neustáleho zlepšovania založený na uznávaných priemyselných normách.
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.	Zásady a postupy informačnej bezpečnosti, úlohy, zodpovednosti a povinnosti sú stanovené v súlade s obchodnými požiadavkami DODÁVATEĽA a príslušnými zákonmi a predpismi. Zásady informačnej bezpečnosti schvaľuje vedenie, sú zverejnené a oznámené zamestnancom a príslušným externým stranám.
The SUPPLIER regularly reviews its compliance to established security policies, standards and any other security requirements.	DODÁVATEĽ pravidelne overuje, či dodržiava stanovené bezpečnostné politiky, normy a všetky ostatné bezpečnostné požiadavky.
Risk Management	**Riadenie rizík**
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.	DODÁVATEĽ má zavedené riadenie bezpečnostných rizík. DODÁVATEĽ zabezpečí, aby sa posúdili riziká, ktoré priamo alebo nepriamo ovplyvňujú služby a/alebo údaje ZÁKAZNÍKA, a aby sa zaviedli a zdokumentovali opatrenia na ich zmiernenie. Riziká, ktoré priamo alebo nepriamo ovplyvňujú ZÁKAZNÍKA, musia byť na požiadanie nahlásené.
Contractual Agreement	**Zmluvná dohoda**
The SUPPLIER must include responsibilities for information security in contractual agreements with their employees and contractors.	DODÁVATELIA musia zahrnúť zodpovednosť za bezpečnosť informácií do zmluvných dohôd so svojimi zamestnancami a dodávateľmi.
Background Checks	**Background -kontroly**
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.	Kontroly uchádzačov o zamestnanie sa vykonávajú v súlade s príslušnými zákonmi a predpismi. Rozsah kontroly musí byť primeraný riziku spojenému s úlohou žiadateľa.
Awareness Program	**Program zvyšovania informovanosti**
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 employees must have adequate skills related to their roles and responsibilities.	Všetci zamestnanci DODÁVATEĽA a v prípade potreby aj dodávatelia absolvujú školenie, ktoré zodpovedá ich úlohe. Okrem toho budú zamestnanci informovaní aj o aktualizáciách zásad a postupov DODÁVATEĽA. Všetci zamestnanci musia mať potrebné vedomosti na plnenie svojich povinností a zodpovedností.
ICT Project and Change management	**Riadenie projektov a zmien v oblasti ICT**
Asset Lifecycle	**Životný cyklus majetku**
The SUPPLIER ensures that information security is an integral part of information systems across their entire lifecycle (acquisition to decommission of assets).	DODÁVATEĽ zabezpečuje, aby bezpečnosť informácií bola neoddeliteľnou súčasťou informačných systémov počas celého ich životného cyklu (od nadobudnutia až po vyradenie aktív).

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.	DODÁVATEĽ zabezpečí, aby poskytnutý softvér bol podporovaný operačnými systémami a middleware (napr. Java), ktoré dostávajú bezpečnostné aktualizácie a nie sú zastarané. DODÁVATEĽ zabezpečí pravidelné a včasné bezpečnostné aktualizácie počas celej doby platnosti zmluvy.
Software Change Management	**Riadenie zmien softvéru**
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.	DODÁVATEĽ musí mať formálne politiky pre riadenie zmien a bezpečný životný cyklus vývoja softvéru, ktoré tiež špecifikujú kontroly súvisiace s bezpečnosťou. Súčasťou procesov musí byť preskúmanie kybernetickej bezpečnosti nových návrhov systémov alebo zmien systémov a testovanie bezpečnosti pred nasadením. Zmeny sú pred uvedením do výroby náležite vyžiadané, autorizované, testované a schválené.
Secure Software Development Lifecycle	**Životný cyklus bezpečného vývoja softvéru**
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.	DODÁVATEĽ zahrnie aspekty bezpečnosti informácií do dokumentácie výrobku. Táto dokumentácia musí obsahovať pokyny na konfiguráciu služby a/alebo prostredia na zabezpečenie bezpečnej prevádzky. Vyvinutý softvér sa pred sprístupnením ZÁKAZNÍKOVI testuje v kontrolovanom prostredí s cieľom odhaliť zraniteľnosti.
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 thirdparty 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.	DODÁVATEĽ zabezpečí, aby životný cyklus vývoja softvéru obsahoval primerané bezpečnostné opatrenia (Secure Software Development Lifecycle). To zahŕňa okrem iného: -Používanie medzinárodne uznávaných bezpečných metodík vývoja softvéru (vrátane agilných procesov, ako sú Scrum, Kanban atď.) ako neoddeliteľnú súčasť zabezpečeného vývoja softvéru -Bezpečné smernice pre kódovanie založené na medzinárodných normách. -je zaručená integrita zdrojového kódu - Pravidelné vykonávanie bezpečných revízií kódu (statické a dynamické testy zabezpečenia aplikácií) -Skenovanie zraniteľnosti, ktoré zahŕňa aj kódy používané tretími stranami a open source komponenty (napr. knižnice) -penetračné testy vykonané nezávislou treťou stranou -Vhodné školenia pre interných a externých vývojárov softvéru Zistené a známe zraniteľnosti sa opravujú pred uvoľnením do produkcie.

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.	DODÁVATEĽ musí mať jasné zmluvné dohody so všetkými subdodávateľmi služieb s cieľom stanoviť ich zodpovednosť za bezpečnosť ÚDAJOV KLIENTA, ktoré spracúvajú/uchovávajú/prenášajú v mene KLIENTA. DODÁVATEĽ zabezpečí, aby bezpečnostné opatrenia zavedené SUB-DODÁVATEĽMI boli minimálne na úrovni uvedenej v tomto dokumente a v hlavnej zmluve. DODÁVATEĽ overuje účinnosť opatrení v rámci svojho procesu riadenia dodávateľov.
Information Security	**Bezpečnosť informácií**
Identity and Access Management	**Identity and Access Management**
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.	DODÁVATEĽ zaviedol kontroly prístupu na overenie totožnosti a obmedzenie prístupu na oprávnených používateľov. Prístupové práva sú založené na princípoch "need to know" a "least privilege." Okrem toho sa dodržiava zásada "separation of duties".
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	DODÁVATEĽ zaviedol autentifikačné mechanizmy na ochranu prístupu do systémov v súlade s osvedčenými postupmi, ktoré zahŕňajú okrem iného tieto prvky -Zásady používania hesiel (minimálna dĺžka, zložitosť, zamedzenie opakovaného používania). -jedinečná identifikácia používateľa (vyhýbame sa všeobecným a zdieľaným používateľom) -Bezpečné ukladanie/správu/prenos poverení.
SUPPLIER ensures that accounts which are used for access over the internet are protected by strong authentication mechanisms (e.g. multi-factor authentication).	DODÁVATEĽ zabezpečí, aby účty používané na prístup cez internet boli chránené silnými autentifikačnými mechanizmami (napr. viacfaktorová autentifikácia).
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).	DODÁVATEĽ zaviedol prísne kontroly privilegovaných účtov (napr. správcov systému) prostredníctvom silnej autentifikácie, obmedzenia na minimum a prísne monitorovaného používania (napr. viacfaktorová autentifikácia).
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.	DODÁVATEĽ v pravidelných intervaloch preskúma prístupové práva svojich zamestnancov a v prípade potreby ich upraví (t. j. obmedzí/zruší).

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.	DODÁVATEĽ pravidelne analyzuje systémy (operačné systémy, aplikácie, sieťové komponenty) na známe zraniteľnosti. Záplaty sa aplikujú konzistentným, štandardizovaným spôsobom a sú prioritizované podľa ich kritickosti. Ak sa hlavnú príčinu zraniteľnosti nepodarilo odstrániť v primeranom čase, musia sa zaviesť alternatívne opatrenia na zmiernenie rizika, kým sa hlavná príčina neodstráni. DODÁVATEĽ zaviedol proces núdzových zmien.

Network Security	Zabezpečenie siete
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.	DODÁVATEĽ implementoval a udržiava komponenty sieťovej bezpečnostnej infraštruktúry, ako sú firewally, systémy na detekciu/prevenciu narušenia (IDS/IPS) a iné bezpečnostné kontroly, ktoré zabezpečujú detekciu, nepretržité monitorovanie a obmedzovanie toku sieťovej prevádzky s cieľom pomôcť obmedziť vplyv útokov. Pre systémy s vyššou úrovňou rizika (napr. externe vystavené) musia mať zavedené prísnejšie opatrenia.
The SUPPLIER ensures that a formal remote access policy is in place.	DODÁVATEĽ zabezpečí, aby bola zavedená formálna politika vzdialeného prístupu.
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.	DODÁVATEĽ zabezpečí segregáciu a segmentáciu prostredí podľa priemyselných noriem, keď: (1) prostredia sú zdieľané s inými zákazníkmi; a/alebo (2) DODÁVATEĽ implementuje testovacie, kvalitatívne a výrobné prostredie.
Encryption	**Šifrovanie**
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).	DODÁVATEĽ zabezpečí primeranú ochranu dôvernosti údajov. DODÁVATEĽ zváži aj osobitné opatrenia pre údaje pri prenose a v nestálom a trvalom úložisku, ako napríklad používanie šifrovacích technológií v kombinácii s vhodnou architektúrou správy kľúčov. Šifrovanie je v súlade s poprednými normami a usmerneniami alebo ekvivalentnými normami (napr. Národný inštitút pre štandardy a technológie - 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.	DODÁVATEĽ ochráni mobilné zariadenia a externé elektronické médiá (napr. USB pamäť, pásky) pred neoprávneným prístupom prostredníctvom vhodných fyzických a logických bezpečnostných opatrení. bezpečnostné opatrenia proti neoprávnenému prístupu. Musí sa zabezpečiť šifrovanie údajov uložených v týchto zariadeniach.

Malware Protection	Ochrana pred škodlivým softvérom
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.	DODÁVATEĽ je povinný chrániť servery a koncové zariadenia primeranou ochranou proti škodlivému softvéru, ktorá musí byť vždy aktualizovaná. Softvér zisťuje, či je antivírusový/malvérový softvér v zariadeniach vypnutý alebo či nie je pravidelne aktualizovaný.
Security Testing, Monitoring & Reporting	**Testovanie bezpečnosti, monitorovanie a podávanie správ**
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).	DODÁVATEĽ má primerané bezpečnostné opatrenia (najmä s ohľadom na kybernetické hrozby) pre údaje, aplikácie a systémy. DODÁVATEĽ pravidelne vyhodnocuje účinnosť bezpečnostných opatrení s ohľadom na známe kybernetické hrozby a prípady podvodov, ako aj zodpovedajúce modely (napr. na základe aktuálnych katalógov hrozieb, ako je Národný inštitút pre štandardy a technológie, Spolkový úrad pre informačnú bezpečnosť).
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.	DODÁVATEĽ pravidelne plánuje a vykonáva posúdenie zraniteľnosti a penetračné testy systémov používaných na poskytovanie služieb ZÁKAZNIKOVI. Penetračné testy týchto systémov sa musia vykonávať nasledujúcim spôsobom: (1) aspoň raz ročne (2) v prípade významnej verzie/aktualizácie aplikácií/softvéru/informačných služieb. (3) Penetračné testovanie vykonávajú testeri s dostatočnými znalosťami, zručnosťami a skúsenosťami, ktorí sa nepodieľali na vývoji bezpečnostných opatrení. Zistené zraniteľnosti a ich výsledky sa primerane spravujú: Analýza, klasifikácia a náprava. Nápravné opatrenia sa musia vykonať včas v súlade s ich sa vykonávajú včas podľa ich kritickosti. DODÁVATEĽ na požiadanie sprístupní súhrnné správy o posúdení zraniteľnosti a/alebo sa sprístupnia penetračné testy.
The SUPPLIER ensures that security issues identified and reported by the CUSTOMER are resolved within a reasonable timeframe.	DODÁVATEĽ zabezpečí, aby sa odstránili bezpečnostné problémy nahlásené ZÁKAZNÍKOM v primeranej lehote.
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.	ZÁKAZNÍK si vyhradzuje právo vykonať bezpečnostné posúdenie s cieľom overiť súlad s požiadavkami stanovenými v tomto dokumente. ZÁKAZNÍK je povinný vopred informovať DODÁVATEĽA a zabezpečiť, aby sa audit vykonal počas bežnej pracovnej doby a s minimálnym narušením činnosti DODÁVATEĽA. DODÁVATEĽ je povinný na požiadanie písomne potvrdiť splnenie požiadaviek uvedených v tomto dokumente a písomne odpovedať na všetky otázky, ktoré môže ZÁKAZNÍK položiť DODÁVATEĽOVI v súvislosti s jeho bezpečnostné postupy v písomnej forme.

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.	DODÁVATEĽ nakonfiguroval a nasadil svoje IT zdroje (napr. databázy, aplikácie, operačné systémy, sieťové zariadenia) na bezpečnom základe (hardening). Základné bezpečnostné postupy vychádzajú z osvedčených postupov (napr. noriem CIS) alebo rovnocenných postupov. Konfigurácie prostriedkov IT sa pravidelne kontrolujú a aktualizujú.

ICT Operations	Prevádzka IKT
Data Management	**Správa údajov**
The SUPPLIER ensures that measures against data loss and leakage are in place.	DODÁVATEĽ zabezpečí prijatie opatrení proti strate a úniku údajov.
The SUPPLIER must not replicate CUSTOMER production data or use it in non-production environments. Any use of customer data in nonproduction environments requires explicit, documented approval from the CUSTOMER.	DODÁVATEĽ nesmie replikovať produkčné údaje ZÁKAZNÍKA ani ich používať v neprodukčných prostrediach. Akékoľvek použitie údajov zákazníka v neprodukčných prostrediach si vyžaduje výslovný, zdokumentovaný súhlas ZÁKAZNÍKA.
Backup & Recovery	**Zálohovanie a obnovenie**
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.	DODÁVATEĽ zabezpečí, aby existovali koncepcie zálohovania a uchovávania údajov pre každú príslušnú platformu/komponent, za ktoré zodpovedá DODÁVATEĽ. Vykonávajú sa zálohy, doby uchovávania a testy obnovy. Koncepcie zálohovania a postupy obnovy sú vhodné na zaručenie dohodnutých úrovní dostupnosti.
Logging & monitoring	**Protokolovanie & monitorovanie**
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.	DODÁVATEĽ prijal vhodné opatrenia na zabezpečenie zodpovednosti a vysledovateľnosti vykonaných operácií. Protokoly musia obsahovať dostatok informácií na identifikáciu príčiny (bezpečnostného) problému a umožniť obnovu série udalostí. Protokoly sa musia sprístupniť ZÁKAZNÍKOVI, ak má ZÁKAZNÍK oprávnené dôvody. Do protokolov sa musia zaznamenávať pokusy o prístup, informácie o udalostiach zabezpečenia systému a siete, varovania, zlyhania a chyby. Musí byť zaručená integrita súborov denníka. Prístup k súborom s logmi musí byť obmedzený.
Incident Management & Reporting	**Riadenie incidentov & 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.	DODÁVATEĽ musí mať zdokumentované postupy týkajúce sa incidentov informačnej bezpečnosti, ktoré umožňujú účinné a správne riešenie bezpečnostných incidentov. Postupy zahŕňajú hlásenie, analýzu, monitorovanie, riešenie a dokumentáciu bezpečnostných incidentov.

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.	DODÁVATEĽ je povinný bezodkladne informovať ZÁKAZNÍKA, keď sa dozvie o akomkoľvek incidente, ktorý priamo alebo nepriamo súvisí so službami a údajmi ZÁKAZNÍKA, a poskytnúť všetky dostupné informácie, aby pomohol ZÁKAZNÍKOVI pri plnení jeho povinností. DODÁVATEĽ poskytne tieto informácie postupne, ako budú k dispozícii. Po preskúmaní bezpečnostného incidentu, ktorý sa týka služieb alebo údajov ZÁKAZNÍKA, DODÁVATEĽ: i. písomne informovať obchodné jednotky ZÁKAZNÍKA a dodatočne kontakty definované v zmluve a v časovo kritických prípadoch alebo pri hroziacom nebezpečenstve bez zbytočného odkladu zavolať aj Help-Desk R-IT.
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 subcontractors	ii. Oznámenie musí obsahovať aspoň tieto informácie, ak nie sú všetky informácie spočiatku k dispozícii, DODÁVATEĽ by mal poskytnúť podrobnosti alebo oznámiť bezprostredné nebezpečenstvo hneď, ako sa o nich dozvie v rámci postupného hlásenia: • Kontaktné údaje osoby DODÁVATEĽA, ktorý je zodpovedný za incident. • Čo sa stalo? • Ako sa to stalo? • Prečo sa to stalo? • Ovplyvnené komponenty/zariadenia • Ovplyvnené služby/údaje KLIENTA • Dátum a čas vzniku incidentu • Dátum a čas zistenia incidentu Vplyv na podnikanie / vplyv na služby/údaje ZÁKAZNÍKOV • Riešenie incidentu • Opatrenia prijaté na vyriešenie incidentu • Plánované opatrenia na vyriešenie incidentu iii. Vyvinúť všetko primerané úsilie na prevenciu a odhalenie takýchto incidentov; iv. informovať ZÁKAZNÍKA o opatreniach, ktoré DODÁVATEĽ prijal alebo plánuje prijať; v.získať predchádzajúci písomný súhlas ZÁKAZNÍKA v súlade s platnými právnymi predpismi v súvislosti s akýmkoľvek oznámením alebo zverejnením informácií týkajúcich sa takéhoto porušenia; a vi. koordinovať všetky ďalšie činnosti s ZÁKAZNÍKOM. vii. táto oznamovacia povinnosť sa vzťahuje aj na subdodávateľov.
Physical Security	**Fyzická bezpečnosť**
Physical Access	**Fyzický prístup**
The SUPPLIER has categorized its premises into different protection zones, reflecting certain security measures and access rights according to the relevant security needs.	DODÁVATEĽ rozdelil svoje priestory do rôznych ochranných zón, ktoré odrážajú špecifické bezpečnostné opatrenia a prístupové práva podľa príslušných bezpečnostných požiadaviek.

Access to IT systems such as servers is further restricted with special protection zones for authorized personnel only.	Prístup k IT systémom, ako sú servery, je ďalej obmedzený špeciálnymi ochrannými zónami, do ktorých majú prístup len oprávnení pracovníci.
Only secure data center facilities must be used to store CUSTOMER data.	Na ukladanie údajov ZÁKAZNÍKA sa môžu používať len bezpečné dátové centrá.

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.	DODÁVATEĽ má aktualizované a udržiavané plány obnovy po havárii a plány kontinuity činnosti. Plány obnovy po havárii a plány kontinuity činnosti musia byť navrhnuté tak, aby v maximálnej možnej miere zabránili negatívnym vplyvom neplánovaných prerušení a aby zabezpečili, že DODÁVATEĽ môže pokračovať vo svojej činnosti aj po prerušení prevádzky a naďalej poskytovať Služby, ako je uvedené v jeho zmluve so ZÁKAZNÍKOM. DODÁVATEĽ poskytne ZÁKAZNÍKOVI na požiadanie písomné zhrnutia svojich plánov obnovy po havárii a plánov kontinuity činnosti.
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.	DODÁVATEĽ vykoná aspoň raz ročne primerané testy svojich vlastných plánov kontinuity prevádzky a obnovy po havárii. Výsledky testov relevantných pre servis sa ZÁKAZNÍKOVI sprístupnia na požiadanie, minimálne však po vykonaní testov.
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.	DODÁVATEĽ zabezpečil, aby rozsah plánov kontinuity činností a plánov obnovy po havárii zahŕňal všetky miesta, personál a informačné systémy používané na vykonávanie alebo poskytovanie služieb pre ZÁKAZNÍKA.