BEZPEČNOSTNÍ PRAVIDLA / *SECURITY RULES*

Creditinfo Soutions s.r.o.

1. DATOVÁ CENTRA

1.1. Infrastruktura

Servery jsou umístěny buď v datacentru v pronajatých rackových stojanech nebo v cloudovém prostředí poskytovaném mezinárodními společnostmi (např. Microsoft Azure, Amazon Web Services atd.).

1.2. Redundance

Při umístění serverů v datacentrech jsou uplatňována standardní opatření pro zajištění redundance, zejména:

- Zálohový zdroj napájení
- Zálohové připojení k síti internet
- Virtualizace clusterů s n+1 hosty a přepínači

Pokud jsou zdroje získávány od mezinárodních společností poskytujících cloudové technologie, pak je redundance zajištěna a poskytována těmito společnostmi jako standardní součást placené služby.

1.3. Napájení

Jak je uvedeno výše, tato oblast obecně závisí na vybraném typu datacentra. Vždy musí být zajištěna níže uvedená minimální úroveň:

- Ochrana proti výpadku proudu transformátorovými stanicemi včetně pojistek
- Diesel generátory k překonání dlouhodobého výpadku proudu
- UPS záložní jednotky s oddělenými bateriovými moduly k překonání krátkodobého výpadku proudu

1.4. Operační systémy serveru

CRKI zajišťuje svoji činnost zejména na základě produktů Microsoft, ve většině případů tak bude používán MS Windows Server OS. Konkrétní verze se liší s ohledem na

1. DATA CENTRES

1.1. Infrastructure

Servers are placed either in the datacenter within rented racks or in cloud environments provided by international companies (e.g. Microsoft Azure, Amazon Web Services etc.).

1.2. Redundancy

When servers are in datacenters, then standard redundancy measures are put in place, mainly:

- Redundant power supply
- Redundant internet connection
- Cluster virtualization with n+1 hosts and switches

When resources are purchased from international companies providing cloud technologies, then redundancy is managed by them and provided already as standard part of the paid service.

1.3. Power

In general, as described in previous point, this dependent on the chosen data center. Nevertheless, the following minimum must be guaranteed:

- Protection against power outages by transformer stations including circuit breakers
- Diesel generators to overcome a longer power outage
- UPS units with separate battery modules to overcome a shorter power outage

1.4. Server Operating Systems

CRKI is mainly a Microsoft based company, so in most of the cases MS Windows Server OS is used. Versions are dependent on the solution, nevertheless it must be always

řešení, vždy však musí být systém pořízen na základě odpovídající licence včetně zajištění dodatečných updatů.

Pokud jsou zdroje získávány od mezinárodních společností poskytujících cloudové technologie, licence pro operační systémy jsou standardně součástí placené služby.

1.5. Zachování provozu

CRKI je odpovědná za vytvoření a udržování aktuálních plánů k zachování provozu ohledně vybraných středních a vysokých hrozeb pro hostovaná řešení na jejich vlastních serverech. Součástí každého plánu bude popis povinností, situací vedoucích k zahájení postupů podle plánu, popis kritických/mimořádných situací, reportovací metody a popis činností jednotlivých osob v průběhu řešení kritické/mimořádné situace.

2. SÍTĚ A PŘENOS

2.1. Přenos dat

CRKI zajišťuje ve spolupráci s Uživatelem ochranu přenosu dat. Uvedené je zajištěno minimálně využitím firewall řešení, které je nejdůležitějším aspektem víceúrovňového přístupu v oblasti zabezpečení sítí. Smyslem Firewall je filtrovat internetový provoz za účelem zmírnění rizik a ztrát spojených s bezpečnostními hrozbami, při současném zajištění odpovídající úrovně dostupnosti uživateli.

Firewall bude (přinejmenším) zajišťovat následující bezpečnostní služby:

- Kontrola přístupů mezi důvěryhodnými vnitřními a neznámými vnějšími sítěmi
- Blokovaní nevyžádaného provozu dle nastavených pravidel Firewall
- Utajení informací před sítí Internet, jako jsou systémová jména, síťové topologie a ID vnitřních uživatelů
- Logování provozu do a z vnitřní sítě
- Poskytování zabezpečeného VPN připojení (pokud je použitelné a vyžadované)

2.2. External Attack Surface

Hostovaná řešení CRKI jsou chráněna proti externím útokům odpovídajícím Firewall řešením včetně pokročilých rozšíření (např. webová aplikace firewall, GEO IP filtering,

correctly licensed and covered by software assurance for further updates.

When resources are purchased from international companies providing cloud technologies, licenses for OS are already standard part of the paid service.

1.5. Business Continuity

CRKI is responsible for making and keeping up-to-date relevant continuity plans for all selected medium and high-risk threats to hosted solutions on its own servers. Part of each continuity plan must be description of responsibilities, situations which are impulse for initiation of such plan, description of critical/emergency situation, report method and description of personal activities during critical/emergency situation solving.

2. NETWORKS AND TRANSMISSION

2.1. Data Transmission

CRKI in cooperation with the User ensures the data transmission security. This is by minimum done via firewall solution, which is top element of a layered approach in network security. The purpose of such Firewall is to filter Internet traffic in order to mitigate risks and losses associated with security threats, while maintaining appropriate levels of access for users.

The firewall will (at minimum) perform the following security services:

- Access control between the trusted internal network and untrusted external network
- Block unwanted traffic as determined by the firewall rule set
- Hide information, such as system names, network topologies, and internal user IDs, from the Internet
- Log traffic to and from the internal network
- Provide virtual private network (VPN) connectivity (if applicable and required)

2.2. External Attack Surface

Hosted solutions by CRKI are protected against external attacks with appropriate Firewall solutions including advanced extensions (e.g. Web application firewall, GEO IP

Botnet filtering atd.), pokud jsou použitelná a vyžadovaná. Pokud jsou zdroje získávány od mezinárodních společností poskytujících cloudové technologie, je využito stejné nebo vyšší úrovně ochrany.

2.3. Zjištění narušení

Hostovaná řešení CRKI jsou chráněna proti narušení odpovídajícím Firewall řešením včetně pokročilých rozšíření (např. webová aplikace firewall, GEO IP filtering, Botnet filtering atd.), pokud jsou použitelná a vyžadovaná. Pokud jsou zdroje získávány od mezinárodních společností poskytujících cloudové technologie, je využito stejné nebo vyšší úrovně ochrany.

2.4. Reakce na bezpečností incidenty

CRKI je odpovědné za monitorování a řešení všech bezpečnostních incidentů a zranitelností ohledně hostovaných řešení. Každý incident musí být zaznamenán v odpovídajícím systému a roztříděn podle závažnosti. Uvedený postup bude popsán ve vnitřních směrnicích (standardně v rámci dokumentace k ISO 27001, pokud je dostupná).

2.5. Šifrovací technologie

Hostovaná řešení CRKI, která jsou vystavena síti internet, budou k přenosu dat týkajících se chráněných informací vždy primárně využívat šifrovaný HTTPS protokol. Pokud jsou zdroje získávány od mezinárodních společností poskytujících cloudové technologie, je využito stejné nebo vyšší úrovně ochrany.

3. PŘÍSTUPY A KONTROLA

3.1. Kontrola zabezpečení provozu datového centra

Pokud jsou servery CRKI umístěny v pronajatých rackových stojanech, jsou tyto stojany uzamčeny a přístup k nim je umožněn jen oprávněným osobám. Okolí datacentra musí být hlídáno kamerovým systémem a každý fyzický přístup musí být zaznamenán.

3.2. Postupy při fyzických přístupech k datovým centrům

Záleží na tom, zda je datacentrum provozováno s nepřetržitou podporou na místě, která monitoruje veškeré fyzické přístupy a odemyká stojany po identifikaci oprávněné osoby. Pokud je datacentrum provozováno bez takovéto podpory, pak jsou zpravidla uplatňována další bezpečnostní opatření jako: přístup na základě kontroly

filtering, Botnet filtering etc.) if applicable and required. When resources are purchased from international companies providing cloud technologies, similar or higher protection is also applied.

2.3. Intrusion Detection

Hosted solutions by CRKI are protected against intrusion incidents with appropriate Firewall solutions including advanced extensions (e.g. Web application firewall, GEO IP filtering, Botnet filtering etc.) if applicable and required. When resources purchased from international companies providing cloud technologies, similar or higher protection is also applied.

2.4. Incident Response

CRKI is accountable for monitoring and solving all security incidents and vulnerabilities regarding the hosted solutions. Each incident has to be recorded in appropriate system sorted out without delay based on the incident severity. Such process should be described in internal guidelines (usually within ISO 27001 documentation if applied).

2.5. Encryption Technologies

Hosted solutions by CRKI which are exposed to internet should always primarily use crypted HTTPS protocol for data transfers of all confidential information. When resources purchased from international companies providing cloud technologies, similar or higher protection is also applied.

3. ACCESS AND SITE CONTROLS

3.1. On-site Data Center Security Operation

When CRKI's servers are placed in the datacenter within rented racks, these racks need to be locked and accessible only by authorized persons. The perimeter of datacenter must be monitored by video surveillance system and all visits must be logged.

3.2. Data Center Access Procedures

Depends if the datacenter is with 24/7 technical on-site support which then monitor all visits and unlocks the racks after the identification of authorized person. If datacenter is self-managed, then usually additional security measures appliers such as: finger print access to datacenter

otisku prstů, pokročilé monitorování kamerovým systémem s využitím dálkové přítomnosti bezpečnostní služby atd.

3.3. Zabezpečení zařízení nacházejících se v datovém centru

Pokud jsou servery CRKI umístěny v pronajatých rackových stojanech, tyto stojany nedovolují připojení žádných externích zařízení neoprávněnými osobami. Každé zařízení musí mít štítek s vlastním ID a musí být zapsáno v seznamu umístěných zařízení. Bez vědomosti oprávněných osob odpovědných za umístěná zařízení není možné přinášet nebo odnášet jakákoli externí zařízení.

3.4. Zabezpečení infrastruktury

Fyzický přístup k serverům a aktivním síťovým prvkům u hostovaných řešení CRKI na jejím vlastním HW je dovolen pouze oprávněným osobám. Místnost se servery a aktivními síťovými prvky je povinně uzamknutá. Místnost je uzamknutá elektronickým zámkem s možností logovaných vstupů, nebo je logování zajištěno odpovědnou osobou.

3.5. Kontrola přístupů

Přístupová práva k hostovaným systémům CRKI jsou přidělována v nejširším možném rozsahu na základě Role-Based Access Control (RBAC). Pouze ve výjimečných případech je možné přidělit přístupové právo prostřednictvím uživatelského účtu. Jednotlivým rolím jsou přidělena pouze nezbytně potřebná práva. Kontrola přístupu je řízena autorizovanými administrátory systému a všechny přístupy musí být vytvořeny nebo měněny pouze na základě schválené žádosti příslušným majitelem příslušného systému (typicky Service Desk).

3.6. Přístupová politika

Následující pravidla musí být dodržována v nejširším možném rozsahu (pokud je to technicky možné). Uživatelské heslo se musí skládat z 8 znaků (nejméně); heslo administrátora se musí skládat nejméně z 12 znaků. Všechna hesla musí být (pokud je to technicky možné) dostatečně komplexní, což je při splnění alespoň 3 z následujících 4 podmínek: 1. velká písmena (A-Z), 2. malá písmena (a-z), 3. čísla (0-9), 4. nenumerické znaky (např. !, $, #, %). Systém musí požadovat změnu dočasně přiděleného hesla při prvním přihlášení. Heslo musí být změněno po určitém časovém období (typicky 90 dní).

4. DATA

perimeter, advanced monitoring via surveillance system with remote security service etc.

3.3. On-site Data Center Security Devices

When CRKI's servers are placed in the datacenter within rented racks, these racks do not allow to connect any external devices by any unauthorized persons. Each device has to be labeled with its own ID and documented in list of placed devices. It is not possible to bring or take any device without the knowledge of authorized personnel responsible for placed HW.

3.4. Infrastructure Security Personnel

Physical access to servers and active network components by CRKI hosted solutions on its own HW is permitted only to competent persons. The room with placed servers and active network components is under regime of obligatory locking. The room is either locked by electronic lock with possibility of entrances logging or logging is done by responsible person.

3.5. Access Control and Privilege Management

Access rights to CRKI hosted systems are assigned by Role-Based Access Control (RBAC) to the greatest extent possible. Only in exceptional situations it is possible to assign access right by user account. To roles are allocated only strictly necessary permissions. Access Control is managed only by authorized System Administrators and all accesses must be created or altered only on basis of approved request by relevant owner in desired system (typically Service desk).

3.6. Access Policy

The following rules shall be applied as much as possible (if technically applicable). User password has to consist of 8 characters (at least); Administrator's password shall contain at least 12 characters. All passwords must fulfill (where technically possible) the requirement on complexity, which is at least 3 of following 4 conditions: 1. capital letters (A to Z); 2. small letters (a to z); 3. numbers (0 to 9); 4. non-alphanumeric character (e.g. !, $, #, %). System has to require the change of temporarily assigned password during first login to the system. Password must be changed after defined period of time (typically 90 days).

4. DATA

4.1. Uložení dat, oddělenost, logování

Každý hostovaný systém CRKI má vlastní oddělené servery (fyzické nebo virtuální). Přístupová práva jsou nastavena za účelem striktní ochrany a oddělení těchto systémů od sebe. Kontrolní záznamy jsou následně nastaveny na serverech CRKI k zaznamenání nastavených privilegovaných operací, monitorování chodu a výpadků systému, všech pokusů o neoprávněný přístup a chyb.

4.2. Postupy při mazání paměťových médií

Při likvidaci a vyřazování zařízení zpracovávajících data je třeba dbát na to, aby všechna paměťová media (např. hard disky počítačů a serverů, paměťové karty s uloženou konfigurací síťových prvků, paměťové karty mobilních telefonů atd.), která obsahují citlivá/chráněná data a data ohledně konfigurace, byla před likvidací nebo vyřazením neobnovitelně smazána. Pokud je elektronické paměťové medium smazáno, musí dojít k přeformátování a přepisu náhodnými daty, minimálně v třech po sobě následujících cyklech. Je vhodné využít specializovaný software, který zajistí požadovaný postup.

Pokud není možné provést bezpečný výmaz nebo je třeba zařízení z rozličných důvodů fyzicky zničit, pak musí být provedena destrukce neumožňující další použití zařízení nebo čtení informací uložených na zařízení. Likvidaci zařízení zajišťuje odpovědná osoba na základě spolupráce se smluvním partnerem.

5. OSOBY

5.1. Chování

Každý uživatel disponuje unikátním přihlašovacím jménem za účelem sledování odpovědnosti jednotlivých osob při vykonávaných činnostech. Sdílení uživatelských jmen není dovoleno. U každého uživatele musí být dodržena pravidla tvoření hesel uvedená výše. Uživatel se vždy musí řídit vnitřními předpisy a bezpečnostními pokyny, které tvoří součást vnitřní dokumentace uplatňované v rámci CRKI (standardně v rámci dokumentace k ISO 27001, pokud je dostupná). Uvedená dokumentace musí zahrnovat alespoň politiku prázdného stolu a obrazovky, pravidla pro užívání SW na koncových stanicích uživatelů, ochranu před škodlivým kódem, pravidla pro nakládání s IT vybavením a pro užívání informačních a komunikačních služeb.

5.2. Školení

4.1. Data Storage, Isolation and Logging

Each hosted CRKI system is having its own separated servers (either physical or virtual). Access rights are then set to strictly protect and isolate such systems from each other. Audit logs are then set-up on CRKI servers to record default privileged operations, monitors the system operation and its outage and all attempts on unauthorized accesses and errors.

4.2. Disk Erase Policy

During the liquidation and removing of devices on the data processing it is needed to observe that all memory medium (e.g. computer and servers hard discs, memory cards with the saved configuration of network elements, cell phones memory cards etc.) which contain the sensitive/secret data and configuration data were before removing or liquidation irrecoverable deleted. When electronic data medium is erased there have to be done reformat and rewriting of random data, minimally in three consecutive cycles. It is convenient to use specialized SW tools which ensure given process.

If it is not possible to do secure erasing or given device has to be physically destroyed from different reasons, then it is needed to do the destruction so that it would not be possible to use given device or to read information from this device. Carrying out the liquidation ensures responsible person through a contractual partner.

5. PERSONNEL SECURITY

5.1. Conduct

Every user has a unique user name in order to be able to trace individual's responsibility for the performed activity. Sharing the user names is not allowed. For each user then has to be applied password policy described above. User has to always follow all defined internal rules and security guidelines which form part of internal documentation applied within CRKI (usually within ISO 27001 documentation if applied). Such documentation should include at least clear desk and screen policy, rules for usage of SW on end user stations, malicious code protection, rules for handling IT equipment and rules for usage of information and communication services.

5.2. Training

Školení ohledně bezpečnostních opatření a pravidel musí být absolvováno všemi zaměstnanci nebo jinými pracovníky nejméně jedenkrát ročně (většinou v rámci ISO 27001 povinného ročního školení).

6. SUBDODAVATELÉ

Fyzický nebo jiný přístup třetích osob (subzpracovatelů) k informačním zdrojům není možný, dokud nejsou zvážena všechna rizika tyto zdroje ohrožující. Zjištěná rizika vztahující se k přístupu třetích osob musí být odstraněna odpovídajícími opatřeními. CRKI je odpovědná za identifikaci těchto rizik a návrh opatření. Je nezbytné, aby byl zpracován záznam o přístupu třetích osob, který bude ověřen odpovědnou osobou CRKI.

Ve smlouvách s třetími osobami musí být zahrnuty, připadá-li to v úvahu, následující podmínky:

- Obecná bezpečnostní pravidla
- Popis služeb, které budou přístupné třetím osobám
- Postupy zajišťující návrat všech zdrojů a jejich likvidaci po skončení smluvního vztahu
- Odpovědnost za zabezpečení zdrojů
- Právo monitorování a zákazu aktivit třetím osobám
- Cílová úroveň služeb a neakceptovatelná úroveň služeb
- Podmínky spolupráce s dodavateli třetích osob
- Právo kontroly smluvních povinností s využitím externích auditorů
- Systém hlášení incidentů
- Sankce za porušení pravidel
- Odpovědnosti vycházející z právních požadavků
- Odpovědnost za instalaci, technickou údržbu a za software

Training of the security measures and rules must be completed by all workers at least once a year (this is usually done within ISO 27001 yearly mandatory training).

6. SUBPROCESSORS

A physical or logical access of third parties (subprocessors) to information assets cannot be allowed until all the risks that may threaten these assets are considered. The identified risks related to the access of third parties have to be covered with appropriate measures. CRKI is responsible for the identification of such risks and proposal of measures. It is necessary there exists a record about the access of the third party which is verified by responsible CRKI worker.

In contracts with external parties should be, in cases where it makes sense, included at least the following requirements:

- General information security rules
- Description of the services that will be available to the third party
- Procedures which ensure return of all assets and its disposal after the termination of contractual relation
- Responsibility for the security of assets
- The right to monitor and to prohibit activities of third party
- Target level of service and unacceptable level of services
- Terms of cooperation with third party subcontractors
- The right to audit contractual obligations also through external organizations
- Security incident reporting system
- Penalties for breaking the rules
- Responsibility which arises from valid legal requirements
- Responsibility for installation, technical maintenance and for the software

• Jasně specifikovaná pravidla řízení změn • Popis ověřitelných kritérií plnění a způsobu jejich monitorování	• Clear and specified procedure of change management • Description of a verifiable criteria of performance and a way of their observation
Výše uvedené podmínky pro smlouvy s třetími osobami mohou být splněny uzavřením dohody o mlčenlivosti.	The above described requirements for the contract with the third party may be settled by signing a non-disclosure agreement.