Asseco CEIT, a.s.
info@asseco-ceit.com
Univerzitna 8661/6A, 010 08 Zilina
Slovak Republic
+421 (0)41 513 7401
+421 (0)41 513 9290

Rules for Security Critical Vendors

A Non-Disclosure Agreement (NDA) must be concluded with any security critical vendor, committing it and Asseco CEIT to keep confidential and secure all information, documents and equipment to be provided. Should this agreement be breached by the vendor, it will be obliged to pay contractual penalties and compensate Asseco CEIT for damages caused.
Vendors are required to have an information security management system in place, although it does not have to be certified. Vendors are likewise required:

a) To have established and approved a security policy covering the security of data and information that may be generated and processed by the vendor when it supplies the deliverables indicated in contracts concluded between it and Asseco CEIT. The security policy must contain guiding principles, objectives, security needs, rights and obligations in relation to information security management.
b) To manage inherent risks which may affect the supply of the deliverables.
c) To implement appropriate security measures, based on security needs and the results of a risk assessment, when supplying the deliverables; monitor such measures, and evaluate their effectiveness.
d) To establish processes and technologies for maintenance of up-to-date security measures that comply with the security policy.
e) To register all data and information created and processed when it supplies the deliverables, and record all security-related material circumstances for such data and information, making such registers and records available to Asseco CEIT, a. s. upon its request.
f) To adequately comply these security requirements whenever it engages a subcontractor to supply deliverables and also in its contractual relations with subcontractors.

1 Human resources security

1.1 Security critical vendors and their subcontractors, if any are engaged, are required to take the following action in their internal processes:

a) To have a security awareness development plan in place to ensure adequate training and enhancement of security awareness, which includes the following:
   - Instructing users, administrators, security role persons and subcontractors on their responsibilities and the security policy;
   - Ensuring theoretical and practical training of users, administrators and security role persons;
b) Designating staff responsible for carrying out each of the roles set out in the security plan;
c) Briefing users, administrators, security role persons and contractors on their responsibilities and the security policy through initial and regular training sessions in accordance with the security awareness development plan;
d) Regularly training security role persons in accordance with the security awareness development plan, taking current cybersecurity needs into consideration;

e) Providing staff with regular training and security awareness in tune with their job description and in compliance with the security awareness development plan,;
f) Monitoring of users, administrators and security role persons for compliance with the security policy;
g) Orderly transfer of responsibilities should the contractual relationship with an administrator or security role person be terminated;
h) Establishing rules and disciplinary procedures were a user, administrator or security role person to violate established security rules; and
i) Keeping a record of training sessions including the subject of the session and a list of the persons who have received training.

1.2 Asseco CEITs reserves the right to keep records and verify a vendor's activities, to register incidents and non-standard action taken by employees or any other persons acting on a vendor's behalf. Based on these records, it is entitled to evaluate whether a vendor's employees are trustworthy and reliable. Should there be an identified risk, Asseco CEIT will notify the vendor in question of non-compliance and both parties will negotiate a resolution of the situation.

1.3 A vendor's employees shall be qualified to perform the work and to have been entrusted with the level of security the job position demands.

2 Physical security, fire protection and occupational health and safety

When supplying contracted deliverables a vendor, as an employer, is responsible for compliance by its employees and other natural persons the vendor may engage and contract with occupational safety and health (OSH) and fire protection (FP) regulations. It is likewise responsible for compliance with conditions for the access of these persons to Asseco CEIT premises.

3 Management of IS Operations

Vendors undertake:

a. To guarantee the secure operation of the information system and infrastructure they use to supply contracted deliverables.
b. To provide Asseco CEIT, at its request, with an overview of security measures implemented on the information system and infrastructure through which a vendor supplies contracted deliverables.
c. To ensure that only applications and technologies in compliance with applicable Slovak and European legislation are used to supply the deliverables, especially with regard to licensing conditions, copyright and copyright-related rights and on the amendment of certain laws (Copyright Act), as amended.

4 Access control

4.1 Identification

a. Every person employed by a vendor to supply contracted deliverables through its computing resources is required to have their unique user account registered and maintained within the IT infrastructure and been assigned specific roles in each designated system, module or application. Each vendor employee has to be identifiable with recorded and up-to-date contact information.
b. Every person employed by a vendor with access to Asseco CEIT's internal systems will receive a unique user account created by Asseco CEIT, with specific roles exclusively related to the contracted deliverables assigned in individual systems, modules or applications.

4.2 Authentication

4.2.1 Conditions for authentication when using Asseco CEIT's ICT infrastructure.

a. Multi-factor authentication for uniquely identifying privileged users of designated systems; or
b. Password authentication when multiple factors cannot unambiguously identify privileged users, using cryptographic keys with a guarantee of a similar level of security or the use of a password with the required rules.

4.2.2 Vendors are required to submit supporting documentation for their employees' remote access by completing a remote access request, wherein parameters for secure remote access are then set.

a. Applications are completed internally at Asseco CEIT on the vendor's behalf by whoever is responsible for the designated system (based on input from the vendor's contact person).
b. Once the request has been processed, each of the vendor's employees is familiarised with details of the remote access rules specific to him or her and then given the authentication data.

4.2.3 Vendors are responsible for the actions of its employees and other natural persons engaged or contracted for their benefit and they are required to comply with security rules and other clarifying security information to be provided by Asseco CEIT, at the vendor's request. Any and all damage caused by a vendor's employee or other engaged or contracted person having violated this and/or other security information shall be borne by the vendor, who is then obliged to compensate Asseco CEIT in full for such damage.

4.3 Authorisation

4.3.1 Persons employed by vendors are obliged to use privileged authorizations in Asseco CEIT's ICT infrastructure only to a reasonable extent and strictly for the period necessary to supply contracted deliverables. Neither users nor administrators may use privileged accounts for routine work unrelated to the designated system's administration.

4.3.2 Asseco CEIT will brief persons employed by vendors about whatever protected information they have been granted access to and how it can be handled. Vendors are neither permitted to handle Asseco CEIT's protected information, nor to perform any other operations therewith unless they have been explicitly instructed to do so.

4.4 Remote access conditions

4.4.1 Asseco CEIT's own hardware and software are used by default to access information systems at Asseco CEIT. Any access by a vendor's PCs, laptops or other computing equipment to protected internal information and to information and telecommunication systems has to be approved by both Asseco CEIT's ICT department and the administrator in charge of the system.

4.4.2 VPN-connected vendor workstations are required to have the following:

a. Advanced functional virus protection (with real-time protection enabled);
b. Functional personal firewall;
c. Automatic/managed operating system updates set up;
d. Operating systems not out of service support;
e. Similar Linux environment conditions as defined above for Windows - AV, FW, UPDATE, OS;
f. Identification and authorization elements provided by a designated Asseco CEIT employee stored in the end station;
g. VPN client installed solely at the vendor's expense;
h. The second factor (HW or SMS token) for VPN access, to be provided by the designated staff;
i. Updated third-party apps that do not infringe any copyrights.

5 Change management

Changes made by a vendor should consider the criticality of information, systems, and processes together with a reassessment of risks. In managing the changes, vendors undertake:

a) To record contract changes.
b) To record changes made to the services they provide as recommended in Information Security Standards.

6 Acquisition, development, maintenance

Vendors undertake to safely implement, upgrade, update, and test technologies to be supplied and handed over to Asseco CEIT, and to document at least the following:

a) Real performance;
b) All security settings, functions and mechanisms;
c) Description of the authorization concept and authorization;
d) Backup and archiving procedures;
e) Installation and configuration procedures;
f) Any vulnerability testing and compliance with Asseco CEIT's security requirements;
g) Assurance of business continuity and disaster recovery.

When developing a solution, vendors undertake:

a. To implement best practices for safe software development and to comply with them;

b. To facilitate an audit of the proposed or implemented solution if the delivery of source code is a contracted deliverable, and in particular to verify that the solution fulfills the conditions of the contract;
c. To ensure that the solution includes only those components objectively necessary for it to operate and/or are specified explicitly in the contract (particularly that the solution contains no unnecessary components and no software samples);
d. To install the prescribed versions of products compatible and functional in the environment that exists at Asseco CEIT were the solution to include the installation of an operating system or third-party software;
e. To ensure the vendor's testing environment is secure and to protect test data provided by Asseco CEIT;
f. To deliver only the compiled or executable code contractually specified and any other data necessary for operating the solution in Asseco CEIT's production environment;
g. To guarantee that the delivered solution complies with recommendations in information security standards;
h. To provide customers with the necessary assistance were they to require and/or carry out security testing of the solution. Should a customer require the vendor to confirm safety testing of the solution, it would be agreed in a separate contractual agreement;
i. To deliver the source code to Asseco CEIT, if the contract specifies it, in a secure form and with the assurance of its integrity;
j. To control the source code version;
k. To back up the source code and store it outside the production environment;
l. To ensure that the distributed source code includes a file from the development environment for the controlled compilation of the code;
m. Not to develop, compile or distribute in Asseco CEIT's environment any program code intended for illegal control, or that would either impair availability, confidentiality or integrity or acquire data and information in an unauthorized or illegal manner.

7 Monitoring

a) Access by persons employed by a vendor to selected protected internal information and to Asseco CEIT's information and communication systems will be continuously recorded, monitored and evaluated. Events in the systems are logged by Asseco CEIT;
b) Vendors are required to continuously monitor their ICT infrastructure for disclosed and known security vulnerabilities that may affect the smooth and secure operation of systems related to the services they provide, such as vulnerabilities in operating systems, third-party software, and web components.

8 Media protection

a. Any storage of Asseco CEIT's protected information belonging to on portable media and any transport of media outside of its premises have to be approved by Asseco CEIT;
b. Vendors are obliged, when Asseco CEIT's protected information is stored on portable media, to store or require the storage of such data in encrypted form and to keep records of such media, if technically feasible;
c. Vendors are required to destroy any operational data that contains Asseco CEIT's protected information as soon as there is no longer any purpose for the processing and/or storing it. Such information should no longer be recoverable once data on the electronic medium has been destroyed. Vendors are likewise required to keep a record of any data that has been destroyed.

9 Cyber incidents

Vendors are obliged to report all suspected cyber incidents:

a. To the person employed at Asseco CEIT in charge of resolving them
b. Immediately upon having identified the cyber security event/incident.
c. By email, telephone with call recording on both sides, or in-person
d. Describing the following:
    - Date and time of incident identification;
    - Nature of the event;
    - Source of the event;
    - Targets/victims of the event;
    - Potential impact.

10 Customer audit

10.1 Authorized audits

a. Asseco CEIT reserves the right to audit vendors.
b. Asseco CEIT will notify a vendor of its intention to audit it at least five (5) working days in advance thereof. Both the vendor and Asseco CEIT shall approve the scope and timing of the audit and any necessary cooperation between them, with the understanding that Asseco CEIT will proceed in such a way as not to disrupt the vendor's operational needs.
c. Asseco CEIT reserves the right not to announce an audit of a vendor in connection with contracted deliverables were it to have serious grounds for secrecy, such as suspicion of risky behaviour, while taking into account the vendor's operational situation.
d. Should nonconformities be identified, remedial action in response to the finding would be established and a date set for implementation. The vendor is obliged to take remedial action within the scope of the specified finding and the required timeframe.
e. Audits are documented by Asseco CEIT and recorded by the unit responsible for conducting audits. The same identifier is always used for a particular audit. Each audit file includes the following:
    - Audit plan;

- Announcement of the audit;
- Audit questionnaire (a list of questions to be asked, if deemed appropriate);
- Audit report;
- Written, photographic and other records of relevant operations, procedures and equipment (if necessary to document the findings);
- Recorded findings (including remedial action and follow-up).

f. Audited vendors will receive a final audit report containing any findings for comment:
   - Vendors will propose action and draft deadlines for solutions based on the findings presented in the final audit report, submitting a list of them to Asseco CEIT for its approval;
   - Asseco CEIT will confirm its approval of proposed action.

10.2 Remedial action

a. Audited vendors are required to take any agreed remedial action within a specified time; and
b. Audited vendors will communicate and hand over reports on action taken to Asseco CEIT.

11 Protecting assets against unauthorized activities

Vendors are prohibited from installing and using tools on Asseco CEIT assets that have not been specifically contracted by Asseco CEIT.

12 Conditions for termination of the contract

a. Should a contractual relationship be terminated, all access by the vendor and its employees to Asseco CEIT assets such as its VPN, systems and information must be likewise terminated no later than the date of the contractual relationship's termination.
b. Any Asseco CEIT assets provided to a vendor's employees have to be returned no later than the date of the contractual relationship's termination.
c. Any information assets or data a vendor has provided to Asseco CEIT must be returned and purged, with no possibility of recovery from any of the vendor's and media, no later than on the date of the contractual relationship's termination.
d. Should the contractual relationship be terminated early other than by supplying deliverables (such as either the vendor or Asseco CEIT terminating or withdrawing from the contract or by them agreeing to terminate it), any access by the vendor may be terminated by Asseco CEIT, if necessary, before the term of the contractual relationship has expired.