Anlage Informationssicherheit

Dieser Anhang beschreibt die Anforderungen an die Informationssicherheit, die von Dienstleistern und Lieferanten (nachfolgend „DuL“) der VINCORION zu erfüllen sind. Die Anforderungen an höhere Security Level Stufen beinhalten auch die Erfüllung der Anforderungen aller vorherigen Stufen.

Informationssicherheitsanforderungen

Security Level 1

1) Es gibt einen zentralen Ansprechpartner für Informationssicherheit. Die Kontaktdaten sind der VINCORION mitzuteilen.
2) Das Personal ist mit dem Umgang von vertraulichen und höher eingestuften Informationen geschult.
3) Informationssicherheitsvorfälle müssen umgehend gemeldet werden, sofern vertraulich oder höher eingestufte Informationen oder IT-Systeme der VINCORION betroffen sind. Das gilt auch für Phishing-Attacken oder dergleichen.
4) Es existiert eine Passwortrichtlinie, die auch entsprechend umgesetzt wird.
5) Datenzugriff auf Informationen der VINCORION ist auf einen minimalen Kreis berechtigter Mitarbeiter eingeschränkt.
6) Räume oder Bereiche beim Dienstleister, in denen Informationen der VINCORION elektronisch verarbeitet oder gespeichert werden, müssen durch geeignete Maßnahmen vor unberechtigten Zutritt geschützt werden.
7) Während der Zusammenarbeit mit der VINCORION dürfen nur Datenträger verwendet werden, die durch die VINCORION freigegeben wurden, sofern diese an die Systeme und Netze der VINCORION angeschlossen werden.
8) Bei der Speicherung von sensiblen Daten auf mobilen Komponenten oder Datenträgern (z.B. Notebooks, mobile Datenträger etc.) sind diese durch aktuelle Verschlüsselungsmechanismen zu sichern.
9) Es wird ein aktueller Virenschutz verwendet.
10) Sollten IT-Systeme oder Datenträger auf denen sich vertrauliche Informationen der VINCORION befinden, repariert oder entsorgt werden, muss sichergestellt werden, dass diese Informationen nicht durch Dritte gelesen oder ausgewertet werden können. Die Vernichtung von Informationen hat nach dem aktuellen Stand der Technik nachweislich zu erfolgen. Gleiches gilt für die Entsorgung von Betriebsmitteln und Datenträgern.
11) Der Austausch von vertraulichen Informationen zwischen den DuL und der VINCORION hat über Datenräume zur erfolgen, die nach aktuellem Stand der Technik auf der Anwendungsebene verschlüsselt sind. Genutzte Datenräume für Projekte werden von der IT vorgegeben.

Security Level 2

12) Das Netzwerk ist entsprechend dem aktuellem Stand der Technik getrennt.
13) Systeme und Anwendungen sind nach aktuellem Stand der Technik gesichert.
14) Der Zugriff auf Systemumgebungen der VINCORION erfolgt über einen sicheren logischen Zugangsschutz und darf nur durch dafür berechtigtes Personal erfolgen.

15) Zugriffsberechtigungen zu Systemen und Informationen der VINCORION werden entzogen, wenn Mitarbeiter der DuL das Aufgabengebiet wechseln oder aus dem Unternehmen ausscheiden. Der Vorgang ist zu dokumentieren und Mitarbeiter-Accounts zu deaktivieren.

Security Level 3

16) Es wird ein systematisches Informationssicherheitsmanagementsystem (ISMS) nach nationalem oder internationalem Standard betrieben.
17) Der Dienstleister hat ein systematisches Update- und Patchmanagement eingeführt.
18) Softwareentwicklung für VINCORION ist nach aktuellen Qualitäts- und Sicherheitsstandards zu betreiben. Weiterhin dürfen keine Funktionen implementiert werden, die Datenabflüsse oder Überwachung durch Dritte ermöglichen.
19) Gelieferte Software ist frei von bekannten Sicherheitslücken. Software wird auf Schadcode untersucht. Der Nachweis der Sicherheitsüberprüfung ist beigefügt. Weiterhin ist die VINCORION darüber in Kenntnis zu setzen, ob Default-Passwörter eingesetzt werden und Hinweise für eine Passwortänderung sind zu geben. DuL stellen sicher, dass alle beteiligten Zulieferer ebenfalls diese IS-Anforderungen erfüllen.
20) Systeme sind nach anerkannten Verfahren zu konfigurieren bzw. parametrisieren. Voreingestellte Kommunikationsprozesse über das Internet über diverse Protokolle haben verschlüsselt zu erfolgen.
21) Sollten vor der Auslieferung von Software Sicherheitslücken bekannt sein, dann sind diese umgehend zu schließen. Sollten im Nachgang Sicherheitslücken erkannt werden, muss der Informationssicherheitsbeauftragte der VINCORION hiervon umgehend in Kenntnis gesetzt werden.
22) Für Administratoren von Anwendungen und Systemen der VINCORION gelten besonderen Regelungen. Es ist vertraglich festzuhalten auf welche Bereiche der IT-Infrastruktur zugegriffen werden darf und auch nur für diese Bereiche Zugriffsrechte einzuräumen. Der Zugriff auf Systemumgebungen der VINCORION darf nur über die Administratoren-Accounts erfolgen. Die VNCORION muss in der Lage sein dies zu überwachen. Die für die Ausführung benötigten Informationen werden den DuL zur Erfüllung seines Dienstleistungsumfangs entsprechend zur Verfügung gestellt.
23) DuL haben die Erbringung der Leistung daran auszurichten, dass die ungestörte und kontinuierliche Leistungserbringung für den Geschäftsbetrieb der VINCORION gewährleistet ist. Hierbei haben DuL alle Maßnahmen zur Aufrechterhaltung der Betriebskontinuität nach aktuellem Stand der Technik zu treffen und umzusetzen. Es ist ein entsprechendes Notfallmanagement zu etablieren.
24.) Der Dienstleister gestattet der VINCORION die IS-Anforderungen im Rahmen von Audits auf Einhaltung zu überprüfen.

Zusätzliche Sicherheitsanforderungen

Anforderungen an Physische Sicherheit

1) Für Mitarbeiter von DuL, die in Kontakt mit besonders vertraulichen Informationen oder Anlagen kommen, kann der Nachweis einer Sicherheitsprüfung erforderlich sein. Das ist individuell vom Bereich Physische Sicherheit zu prüfen.
2) Sollten DuL physischen Zutritt zu Räumlichkeiten der VINCORION haben, dann hat er nur auf die definierten Bereiche und Systeme Zugriff. Hierfür sind für die zur Aufgabenerfüllung benötigten Berechtigungen und Zugriffe auf einen klar definierten Zeitraum zu vergeben. Nach Beendigung des Dienstleistungsvertrages sind alle Zutritts- und Zugriffsberechtigungen zu entziehen. Unter Umständen ist eine entsprechende Sicherheitsüberprüfung – sofern erforderlich – nachzuweisen.

In gewissen Einzelfällen können DuL auch unter Begleitung zu den für die Verrichtung ihrer Tätigkeiten notwendigen Räumen geführt werden. Bei Bereichen, die einem vorbeugenden personellen Sabotageschutz (vpS) unterliegen, ist eine Überwachung durch den Werkschutz oder vpS-überprüften Mitarbeiter vorzunehmen. Gleiches gilt für DuL, die Zutritte zu Serverräumen, Netzwerkschränken oder dem Rechenzentrum haben. Diese werden vom Werkschutz oder eigenem Personal überwacht.

Anforderungen bei Wartungsarbeiten

Unter Wartung fallen alle Servicemaßnahmen, die sich auf Komponenten oder Systeme der technischen IT-Umgebung der VINCORION auswirken. Wartungsarbeiten können Vor-Ort stattfinden oder innerhalb eines Remotezugriffs. Hierunter fallen folgende Maßnahmen:

- Instandhaltungs- und Reparaturarbeiten
- Fehleranalyse- und Fehlerbehebungsarbeiten sowie Störungsbehebung
- Installation von Softwareupdates und Applikationen
- Installation neuer Firmware- oder Betriebssysteme
- System-, Geräte- oder Softwareanpassungen

Alle Systeme, die zur Wartung genutzt werden, müssen einen sicheren logischen Zugangsschutz haben und vor unberechtigten physischen Zugriff geschützt werden. Die von DuL genutzten Systeme / Komponenten sind nur für den Zweck der Wartung zu verwenden. Weiterhin werden DuL verpflichtet nur die von der VINCORION beauftragten Wartungsarbeiten durchzuführen. Es ist strikt untersagt sich Zugang zum Netzwerkbereichen und IT-Systemen zu verschaffen, die nicht gewartet werden müssen. Für Wartungsarbeiten sind ausschließlich Systeme zu verwenden, die anhand von Best-Practice-Vorgaben und nach aktuellem Stand der Technik konfiguriert und gehärtet sind. Die Systeme müssen beim Wartungszugriff über einen aktiven Schadsoftwareschutz verfügen.

Fernwartungszugriffe dürfen nur über die mit dem DuL und der VINCORION in Absprache eingerichteten Fernwartungszugänge realisiert werden. Die Mitarbeiter der DuL, die Fernwartung durchführen, sind namentlich zu benennen. Zugriffe dürfen nur über eine geschützte Verbindung erfolgen.

Anforderungen an CUI-Verarbeitung

DuL, die sog. CUI (Controlled Unclassified Information) im Rahmen der Verträge mit der VINCORION verarbeiten, haben die Vorgaben in Bezug auf Informationssicherheit aus DFARS 252.204-7012, DFARS 252.204-7019, 252.204-7020 und 252.204.7021 zu erfüllen.

Information Security Appendix

This appendix describes the information security requirements that must be fulfilled by VINCORION service providers and suppliers (hereinafter referred to as "SP&S"). The requirements for the higher security levels also include fulfilling the requirements of all previous levels.

Information security requirements

Security level 1

1) There is a central contact person for information security. Contact details are to be communicated to VINCORION.
2) Personnel are trained in handling confidential and higher level information.
3) Information security incidents must be reported immediately if it concerns confidential or higher level information or if the VINCORION IT systems have been affected. This also applies to phishing attacks or similar incidents.
4) There is a password policy, which is correspondingly implemented.
5) Data access to VINCORION information is restricted to a minimal group of authorized employees.
6) Rooms or areas in which VINCORION information is electronically processed or stored at the service provider's premises must be protected from unauthorized access.
7) During the cooperation with VINCORION, only data carriers approved by VINCORION are permitted to be used if they are connected to the systems and networks or VINCORION.
8) When storing sensitive data on mobile components or data carriers (e.g. notebooks, mobile data carriers, etc.), these must be secured using up-to-date encryption mechanisms.
9) Up-to-date virus protection is used.
10) If IT systems or data carriers that contain information from VINCORION need to be repaired or disposed of, it must be ensured that this information cannot be read or evaluated by third parties. Information must be destroyed in a verifiable manner in accordance with the current state of the art. The same applies to the disposal of operating media and data carriers.
11) The exchange of confidential information between SP&Ss and VINCORION must take place via data rooms that are encrypted at the application level in accordance with the current state of the art. Data rooms used for projects are specified by IT.

Security level 2

12) The network is separated according to the current state of the art.
13) Systems and applications are secured according to the current state of the art.
14) Access to VINCORION system environments takes place only via secure logical access protection with access limited to authorized personnel.
15) Access authorizations to VINCORION systems and information are revoked if SP&S employees change their area of responsibility or leave the company. The process must be documented and the employee account deactivated.

Security level 3

16) A systematic information security management system (ISMS) is operated in accordance with national or international standards.
17) The service provider has introduced a systematic update and patch management system.
18) Software development for VINCORION must be carried out according to current quality and security standards. Furthermore, no functions that enable data outflows or monitoring by third parties may be implemented.
19) The software that is delivered is free of known security vulnerabilities. Software is examined for malicious code. Proof of security clearance is attached. Furthermore, VINCORION must be informed if default passwords are used and must be provided with instructions on how to change the password. SP&Ss ensure that all suppliers concerned also fulfil these IS requirements.
20) Systems must be configured and/or parameterized according to recognized procedures. Default communication processes via the internet using diverse protocols must take place in encrypted form.
21) If the software is supplied with known security vulnerabilities, these must be rectified immediately. The VINCORION information security officer must be immediately informed if any security vulnerabilities are identified afterwards.
22) Special regulations have been put in place for the administration of VINCORION applications and systems. It must be contractually defined which areas of the IT infrastructure may be accessed, with access rights only being granted to these areas. Access to VINCORION system environments is only permitted via the administrator accounts. VNCORION must be able to monitor these. The information required for the implementation is to be correspondingly provided to the SP&Ss to enable them to fulfill their scope of services.
23) SP&Ss are to organize their service provision to ensure undisturbed and continuous provision of services for the business operations of VINCORION. In this connection, SP&Ss are to take and implement all measures to maintain business continuity in accordance with the current state of the art. An appropriate emergency management system is to be established.
24) The service provider allows VINCORION to check compliance with the IS requirements as part of audits.

Additional safety requirements

Physical security requirements

1) It may be necessary for SP&S employees who handle particularly confidential information or systems to undergo a security check. This is to be checked individually by the Physical Security division.
2) If SP&Ss have physical access to VINCORION premises, access is limited only to defined areas and systems. The authorizations and accesses required to fulfil tasks must be granted for a clearly defined period of time. All access rights and authorizations must be revoked when the service contract is terminated. If required, evidence of appropriate security clearance must be provided. In certain individual cases, SP&Ss may also be escorted to the rooms necessary for the performance of their tasks. For areas subject to preventive personnel sabotage protection (PPSP), monitoring shall be performed by plant security or PPSP-verified employees. The same applies for SP&Ss who have accesses to server rooms, network cabinets or the computer center. They are monitored by plant security or their own personnel.

Requirements during maintenance works

Maintenance includes all service activities that have an influence on components or systems in VINCORION's IT environment. Maintenance works can take place on site or during remote access. This includes the following activities:

- maintenance and repair work
- error analysis and troubleshooting, as well as fault elimination
- the installation of software updates and applications
- the installation of new firmware or operating systems
- modifications of systems, devices or software

All systems that are used for maintenance must have secure logical access protection and be protected from unauthorized physical access. The systems/components used by SP&Ss are only to be used for the purpose of maintenance. Furthermore, SP&Ss are obliged only to perform the maintenance works commissioned by VINCORION. It is strictly prohibited to gain access to network areas and IT systems that do not require maintenance. Only systems that have been configurated and hardened on the basis of best-practice standards and according to the current state of the art may be used for maintenance works. Systems must be equipped with active malware protection during maintenance access.

Access for remote maintenance may only take place using remote maintenance accesses that have been set up by agreement with the SP&Ss and VINCORION. SP&S employees performing remote maintenance must be named. Access may only take place via a secured connection.

Requirements for CUI

SP&Ss who process so-called CUI (controlled unclassified information) within the scope of contracts with VINCORION must fulfill the conditions relating to information security from DFARS 252.204-7012, DFARS 252.204-7019, 252.204-7020 and 252.204.7021.