KLINIKEN VALENS

IT Datensicherheit / Datenschutz; IN.1183

Vereinbarung betr. Nutzung von IT-Systemen der Kliniken Valens

Dokumentinformationen	
Dokumentenklasse:	Arbeitsdokument
Dokumententitel:	Systemdokumentation
Vertraulichkeitsstufe:	intern
Verfasser:	Christian Stauffacher, Leiter IT
Status:	Freigegeben, 13.4.23
Version	1.1

A. Änderungskontrolle

Version	Autor	Datum	Beschreibung
1.0	Cst	27.02.2023	Finale Version
1.1	Cst	24.03.23	Update Input Harald

B. Inhaltsverzeichnis

1 Management Summary

Dieses Dokument regelt zusammen mit weiteren Bestimmungen betr. Datenschutz und Datensicherheit die Pflichten von externen Lieferanten bzw. Dienstleistern der Kliniken Valens (nachfolgend gesamthaft als «Lieferanten» bezeichnet).

2 Vereinbarung über die Nutzung von KLV IT Systemen durch externe Dienstleister

Diese Vereinbarung gilt ergänzend zu bestehenden Datenschutzbestimmungen- / Erklärungen und den allgemeinen Einkaufsbedingungen (AEB) der Kliniken Valens.

Die Lieferanten sind verpflichtet, Datenschutzvereinbarungen einzufordern, beim KLV Datenschützer via datenschutz@kliniken-valens.ch einzufordern. Die AEB's sind unter https://www.kliniken-valens.ch/wp-content/uploads/2021/11/AEB-KLV-final.pdf abrufbar.

2.1 Zweck und Allgemeines

Diese Vereinbarung regelt die Nutzung, Verantwortung und Haftung der KLV Informatiksysteme und Anwendungen durch Lieferanten, welche im Einverständnis mit den KLV mittels Remote Zugriff (Horizon/VPN) oder via das KLV-interne Netzwerk mit ihren eigenem IT Geräten auf die Informatiksysteme (Arbeitsplatzsysteme, Server, virtuelle Systeme oder Netzwerk-Komponenten) sowie auf die Anwendungen der KLV zugreifen können.

Diese Vereinbarung soll IT-Fehlfunktionen und/oder Schäden vermeiden, die durch menschliches Fehlverhalten (absichtlich oder fahrlässig) und/oder Missbräuche entstehen können. Zudem soll die Integrität, Verfügbarkeit und Vertraulichkeit der Informationen gewährleistet werden.

Verstösse gegen die Vereinbarung können zivilrechtlich und allenfalls auch strafrechtlich verfolgt werden.

2.2 Verpflichtungen

2.2.1 Bei Erteilung von Systemrechten

Je nach System ist es technisch nötig, dass der Lieferant auf «seinem» KLV-Fachserver höhere oder gar höchste, lokale Systemrechte erhält. Dies dient dem Lieferanten dazu seine eigene Kernapplikation zu installieren.

Diese Rechte dürfen nicht für die Installation von irgendwelchen weiteren Applikationen, Tools, Skripten, etc. verwendet werden. Siehe dazu auch Abschnitt «Applikationen».

Jegliche weitere Installation ist Vorgängig bei KLV IT anzufragen und vorgängig durch KLV IT freizugeben. Informationen im Nachhinein sind nicht zulässig, auch wenn Applikationen für Problembehebungen und Fehlersuche benötigt würden.

2.2.2 Virenscanner

Alle Server/Clients der KLV sind mit Virenscannern ausgerüstet. Der Virenscanner darf weder ausgeschaltet, noch um-konfiguriert werden. Anfragen zu notwendigen Anpassungen oder Konfigurationsänderungen sind mit schriftlicher Begründung an den IT der KLV zu richten. Bei Hinweisen des Virenscanners auf (mögliche) Viren ist der Zugriff auf die Systeme der KLV umgehend zu unterbrechen und die IT KLV sofort zu informieren. Der Zugriff ist erst wieder gestattet, wenn die betroffenen IT-Systeme bereinigt, respektive virenfrei sind.

2.2.3 EndPoint Protection

Die vorhandene KLV Endpoint Protection Software darf nicht abgeschaltet, nicht angepasst und nicht anderweitig durch externe Lieferanten manipuliert werden.

2.2.4 Betriebssystem

Manipulation am Betriebssystem, inkl. Netzwerk-Stack und Monitoring sind untersagt, weder die Installation/das Hinzufügen von Features noch deren Entfernen/Deinstallieren.

2.2.5 Applikationen

Die Installation von Fremd-Applikationen sind ohne vorgängige Zustimmung der IT KLV nicht erlaubt.

Nicht erlaubt sind insbesondere Installationen wie z.B.:

- TeamViewer Host
- Wireshark
- Ports Traffice Analiyer
- CCleaner
- „Eraser“
- „DBAN“
- Aircrack-ng
- TCH-Hydra
- Kismet
- Tor-Projekt
- WinSCP
- RAV EndPoint Protection
- OpenOffice, MS Office oder ähnliche Suiten
- Screensaver aller Arten
- Spiele, Audio Dateien, Filme
- Bitcon’s
- VPN Clients aller Arten

Diese Liste ist NICHT abschliessend und dient lediglich zur Verdeutlichung von nicht-erlaubter Software. Es sind auch immer die „Runtime“, bzw. „Portablen“ Versionen damit gemeint.

3 Minimalanforderungen Lieferant

Die Informatiksysteme des Lieferanten müssen mit einem aktuellen Antivirenprogramm inkl. aktuellen Virenschutz-Definitionen ausgerüstet sein. Alle portablen Datenträger wie Disketten, CD-ROMs, USB-Speicher etc. sind vor dem Anstecken oder Öffnen auf allfällige Viren zu prüfen.

4 Kontrolle, Überwachung und Sanktionen

4.1 Kontrolle und Überwachung

Die Informatikabteilung der KLV überwacht die Einhaltung dieser Vereinbarung durch stichprobenartige, anonyme aber auch gezielte, personenbezogene Auswertungen der Protokollierungen.
Bei der Feststellung eines Missbrauches können weitere, detaillierte personen- und firmenbezogene Auswertungen der Protokollierungen vorgenommen werden. KLV verwendet dazu unter anderem das KLV Graylog System.
Diese Massnahmen werden auch bei begründetem Verdacht auf Verletzung der Sorgfaltspflicht durch den Lieferanten und/oder sofern dringender Verdacht auf die missbräuchliche Nutzung des Informatiksystems und der Anwendungen ergriffen.

4.2 Meldung, Sanktionen

KLV IT ist Mitglied der MELANI / NCSC, Bereich kritische Infrastruktur Gesundheitswesen. Jeder Sicherheitsverstoss muss entsprechend gemeldet werden. Sanktionen zivil- oder strafrechtlicher Art bleiben vorbehalten.

5 Personalabwerbung

Der Lieferant verpflichtet sich, die Mitarbeitenden der KLV in keiner Form abzuwerben.

6 Zutritt zu den Räumlichkeiten der Klinik bzw. Standorte

6.1 Namensschild

Der Lieferant ist verpflichtet, auf dem Areal und in den Räumen der KLV gut sichtbar ein Namensschild zu tragen, das er bei der KLV gegen Unterschrift abzuholen hat.

6.2 Alkohol und Rauchen

Der Konsum von alkoholischen Getränken sowie Rauchen ist während des gesamten Aufenthaltes in den Räumen der Klinik verboten. Personen, die sich nicht an dieses Verbot halten, werden verwarnt und im Wiederholungsfall sofort aus den Kliniken verwiesen.

6.3 Schliessungen

Allfällig benötigte Schlüssel sind bei den KLV gegen schriftliche Empfangsbestätigung zu beziehen und gleichentags zurückzugeben. Schlüssel der KLV dürfen die KLV nicht verlassen. Der Lieferant ist verantwortlich, dass die Räume, zu welchen er durch solche Schlüssel Zugang hat, ordnungsgemäss verschlossen werden.

6.4 Klimageräte

Finden die Arbeiten des Lieferanten in klimatisierten Räumen der KLV statt, so ist der Lieferant verpflichtet vor Arbeitsschluss die Klimatisierung auf ordnungsgemässe Funktion zu prüfen; allfällige ungenügende Funktionen oder Fehlfunktionen sind umgehend zu melden. Daraus folgende (Pikett-) Einsätze der IT KLV betreffend Probleme mit dem Klima in entsprechenden Räumen, die auf die fehlende Prüfung des Lieferanten oder dessen Manipulationen zurückgehen, werden dem Lieferanten pro Fall mit pauschal 5'000.- verrechnet.

7 Gender

Dieses Dokument ist bewusst in männlicher Form verfasst. Selbstverständlich sind immer auch die weibliche Form und alle weiteren Formen damit gemeint.

8 Inkrafttreten

Diese Vereinbarung tritt mit Zustimmung des Lieferanten in Kraft. Die Zustimmung gilt als erteilt, wenn die Vereinbarung dem Lieferanten zugestellt worden ist (Mail ist ausreichend) und wenn dieser dagegen nicht innert 5 Tagen seit Zustellung opponiert.

Valens, 13.04.2023

Informatik KLV
Dokument ohne Unterschrift