TKS-
ZUTRITT/ZUGRIFF

TAGESKLINIK SPENGER-SPITAL

ZUTRITTS- & ZUGRIFFSKONTROLLE
LEITLINIE 03

1. Präambel

Für die Umsetzung der medizinischen Versorgung in der „TAGESKLINIK SPENGER-SPITAL“ (im Folgenden abgekürzt TKS) ist es von entscheidender Bedeutung, dass sämtliche beteiligte Personen davon ausgehen können, dass gravierende Risiken für die TKS, die das Überleben gefährden, frühzeitig zu erkennen und geeignete Maßnahmen dagegen umsetzt.

Bei Zugriff, wie auch bei Zutritt gilt der Grundsatz der Betriebsnotwendigkeit. Auf der einen Seite ist zu gewährleisten, dass jede Mitarbeiterin und jeder Mitarbeiter alle zur Aufgabenerfüllung notwendigen Werkzeuge erhält, auf der anderen Seite sind die Privilegien so zu beschränken, dass wissentliche oder unwissentliche Manipulationen in kunden- und fachfremden Arbeitsgebieten unterbunden werden.

2. Angesprochener Personenkreis

Dieses Dokument richtet sich an die Mitarbeiter im Spengerspital, die für die Wartung und Sicherheit zuständig sind. Desweiteren ist anzumerken, dass Hubert Herbert, bei Ausfall oder einem Hackerangriff, diesen Vorfall innerhalb von 3 Stunden der NIS zu melden hat. Sollte Herr Hubert an diesem Tag nicht anwesend sein so ist dies die Aufgabe von Mayer Lena.

3. Anwendungsweise

Dieses Dokument beschreibt eine Methodik zur Etablierung eines Zutrittskonzeptes und -kontrolle, das zur Sicherheit dienen soll, desweiteren soll die Vertraulichkeit und Verfügbarkeit sichergestellt werden. Um dies zu erreichen, gibt es einige Maßnahmen die gesetzt werden müssen (siehe Punkt 4) Wobei die Verfügbarkeit der Daten am Wichtigsten ist, da es passieren kann, dass die Daten von außen verschlüsselt werden und man so nicht mehr auf die Daten des Patienten zugreifen kann. Das oberste Ziel bleibt aber alle Punkte Verfügbarkeit, Vertraulichkeit, Integrität sicherzustellen.

4. Maßnahmen für den sicheren Zutritt

4.1. Regelungen für Wartungs- und Reparaturarbeiten

Bei Wartungsarbeiten innerhalb des IT Raums:
Bei Wartungs und Reperaturarbeiten, die von externen Mitarbeitern durchgeführt werden, bedarf es einer Prüfung(siehe 4.3).

4.2. Vergabe von Zutrittsberechtigungen

Es gibt ausgewählte Personen, die eine Zugriffsberechtigung an dem Tag haben, der Chip dient zur Ausweisung (dieser ist jeden Tag vom Servicedesk abzuholen und abzugeben.) Dazu zählen Franz Bayer, Mayer Friedrich, Gustav Lang, Sissi Berlyngus, es sind immer 2 Personen eingeteilt, bei einen Ausfall dieser Personen werden die 2 anderen Person für diese Aufgabe eingeteilt.

4.3. Beaufsichtigung oder Begleitung von Fremdpersonen in technischen Räumen

Bei Wartungsarbeiten innerhalb des IT Raums:
Bei Wartungs und Reperaturarbeiten, die von externen Mitarbeitern der IT durchgeführt werden, müssen diese vorher geprüft werden und durch den Metalldetektor gehen, um sicherzustellen, dass

sie keine gefährlichen Waffen mit sich führen. Des Weiteren wird die Person von 2 Mitarbeitern begeleitet, wer diese 2 Personen sind, ist am jeweiligen Tag im Intranet einzusehen. Des Weiteren muss nach jeder Wartungs – und Reperaturarbeit des IT – Raumes, das Passwort erneuert werden. In den Räumen gibt es Videokameras und Bewegungssensoren. Um den IT-Raum betreten zu können, braucht man das ok, des Desks (diesen muss man darüber per Freisprechanlage informieren) der dann die Tür entsperrt, dann muss einer Mitarbeiter seinen Chip innerhalb von 20 sec an den Sensor halten und den Code eingeben. Ohne einen Chip oder des oks des ServiceDesks und ohne Passwort kommt man in den Service Raum nicht hinein, bei gewaltsamen Einbruch in den Serverraum, geht automatisch die Alarmanlage los und das Sicherheitspersonal kommt.

Annahme: Das es einen getrennten Gebäudekomplex gibt
Annhame: Das die oben genannten Mittel zur Verfügung stehen

4.4. Schutz der technischen Räume gegen unbefugten Zutritt

Siehe Punkt 4.3

4.5. Brandschutz

Der Serverraum befindet sich in einem Getrennten Gebäudekomplex, der für die Patienten nicht betretbar ist und nur durch eine Zugriffsberechtigung betretbar ist. Zum Schutz des IT – Raumes in dem sich auch unsere Server befinden, bedarf es eines Brandschutzes. Das Gebäude ist mit MasivBeton ausgestattet und im Ernstfall wird das Gebäude so schnell wie möglich geräumt und durch einen Alarm werden die Mitarbeiter darauf aufmerksam gemacht, das sie so schnell wie möglich den Gebäudekomplex verlassen müssen. Nachdem alle Mitarbeiter das Gebäude so schnell wie möglich verlassen haben. Nach Überprüfung der Sicherheit, dass alle Menschen die Räume verlassen habe, wird der Sauerstoffgehalt in den Räumen gesenkt, sodass das Feuer gelöscht werden kann

5. Maßnahmen für den sicheren Zugriff

5.1. Regelungen für eine Mandantenfähigkeit

Die Mandatenfähigkeit dient dazu, dass die Sicherheit der Daten (Benutzerverwaltung) sichergestellt werden kann ohne, dass diese gegenseitigen Einblick in ihre Daten, Benutzerverwaltung und Ähnliches haben. Aufgrund dessen

5.2. Regelungen für die Administrator-Accounts

Es werden maximal 2 Administrator Accounts vergeben, einen an Herrn Berungi und eine an Frau Mayer Helena. Es gibt immer 2 Administrator Accounts, und wenn eine ihre Stelle abtritt oder Verhindert ist wird die Rolle des Admin weitergegeben. Der Admin muss eine Einverständniserklärung unterschreiben, dass er die Daten nur für das Krankenhaus wartet und das er keine personenbezogenen Daten im Internet veröffentlicht. Bei einem Verlust der Daten ist dies dem Beauftragen Hubert Herbert oder Mayer Lena zu melden

5.3. Vergabe von Rollen (RBAC)

Die Vergabe der einzelnen Rollen, werden von den Admins überprüft. Erst nach der Überprüfung im System der Benutzerverwaltung darf die bestimmte Personen einen Account haben.

5.4. Bearbeitung der Zugriffe

Die Zugriffe können nur durch den Admin verändert werden. Dieser muss dazu in das System einsteigen und diese verändern.