MC-KLINIK +ASV

INFOBLATT IT-Sicherheitsrichtlinie

IT-Notfallmanagement

- Verhalten bei IT-Notfällen – Ruhe bewahren & IT-Notfall melden. Lieber einmal mehr als einmal zu wenig anrufen!
- Wichtig ist, den Notfall schnell an die zuständigen Stellen zu melden.
- Beispielsweise an die IT-Sicherheitsbeauftragte und IT-Sicherheitskoordinatoren, Klinikleitung sowie bei kritischen Störungen den IT-Dienstleister vor Ort.
- Nach der Meldung des Notfalls sind unverzüglich die zwingend erforderlichen Sofortmaßnahmen zu ergreifen.
- Brennt beispielsweise ein Serverraum, müssen gefährdete Personen in Sicherheit gebracht, die Feuerwehr benachrichtigt und der Brand gelöscht werden.
- Viele Aufgaben und die beteiligten Rollen sind bereits rechtlich vorgeschrieben, siehe QM-System.
- Zielsetzung des Notfallmanagements ist es zu verhindern, dass die Unterbrechung oder Störung von wichtigen Prozessen die Existenz der medizinischen Versorgungseinrichtung gefährdet.

Daher sollten möglichst rasch die vorbereiteten Kontinuitätspläne aktiviert werden:

- Mitarbeiter ausführlich informieren und den Aktionsplan einbeziehen, Reservesystem mit ePA Daten aktivieren, Rekonstruktion der Datensicherung mit IT-Verantwortlichen vorbereiten.
- Mögliche Terminverschiebung organisieren und Patienten informieren.
- Sobald der Notbetrieb stabil läuft, muss damit begonnen werden, den medizinischen Versorgungsprozess in den Normalbetrieb zurückzuführen.

INFOBLATT IT-Sicherheitsrichtlinie

IT-Notfallmanagement

- Je nach Art des Vorfalls, sind die Räume einzurichten, IT-Systeme und andere Geräte sind wieder in Betrieb zu nehmen.
- Sobald alle Voraussetzungen für einen funktionsfähigen Normalbetrieb erfüllt sind, kann er wieder aufgenommen werden.
- Sind Arbeitsrückstände aufgelaufen, ist für eine gewisse Zeit noch mit Nacharbeiten zu rechnen.
- Unter Umständen sind dafür Überstunden zu leisten oder aber es muss befristet zusätzlich Personalkapazität zur Verfügung gestellt werden.
- Aus Krisen kann und sollte gelernt werden. Wie kam es dazu? Welche Auswirkungen hat es?
- Wie war die Reaktion? Welche Verbesserungsmöglichkeiten gibt es? Und was kann vorbeugend getan werden.
- Diese Fragen sollte ein Bericht des Notfallbeauftragten an die Leitung beantworten.
- Festgestellte Mängel und Verbesserungsmöglichkeiten sollten offen angesprochen und zeitnah behoben werden.
- Bewahren Sie Ruhe – gemeinsam schaffen wir das.
- Die MCSS AG wünscht viel Spaß und Erfolg mit mehr Cybersicherheit und Datenschutz.