عنوان سند

روش اجـــرایی مدون

بیمارستان امام صادق(ع)دلیجان

عنوان: محافظت و امنیت سیستم های ذخیره و بازیابی اطلاعات	**دامنه:کل بیمارستان**

هدف:

- محافظت از کلیه اطلاعات الکترونیکی پرونده های پزشکی در برابر دسترسی های غیر مجاز و جلوگیری از هر گونه سوء مشاهده، سوءاستفاده و تغییر اطلاعات
- کاهش خسارات اطلاعاتی اعم از پاک شدن اطلاعات یا تغیر داده ها و یا ویروسی شدن شبکه IT و افزایش سطح ایمنی نرم افزار HIS جهت ایمنی اطلاعات و قطعات

تعاریف:

- HIS: بمعنی سیستم اطلاعات بیمارستانی و بعنوان نام نرم افزار بیمارستان استفاده میشود.
- SERVER: سیستم مادر و اصلی بیمارستان که کلیه اطلاعات و پردازش بروی اطلاعت را انجام می دهد.
- Domain : نوع ارتباط بین سیستمها
- Client : به هر سیستم در شبکه که فقط کار ارسال و دریافت اطلاعات به سرور را دارد گفته می شود.

- محافظت و امنیت ، سیستم های ذخیره و بازیابی اطلاعات: کلیه فعالیتهایی که انجام می شود تا سیستمهای ذخیره و بازیابی اطلاعات از هر گونه خطری محفوظ بمانند. یعنی حفظ اطلاعات بیماران اعم از سیستمی ، دستی ، و یا رایانه ای در چارچوبی که منشور حقوقی بیمار تعیین کرده است و شامل قوانین دسترسی، استفاده ، افشا ،خواندن ، نسخه برداری ،ضبط ،تغییر و یا دستکاری می باشد.

منابع /مراجع:

- مدارک پزشکی ۳ و ۴
- مدیریت مدارک پزشکی
- اینترنت
- تجربه بیمارستان و کارشناسان

مسئولیت ها و اختیارات:

- مسئول IT
- کارشناس مدیریت اطلاعات سلامت

شیوه انجام کار:

مسئول IT

۱. شبکه اطلاعاتی را بازرسی و تست امنیت می کند
۲. واحد IT جهت جلوگیری از بروز مشکلات از آنتی ویروسها در سیستم استفاده می نماید
۳. با نصب آنتی ویروس مطمئن برروی سرور از نفوذ احتمالی ویروس به سرور و پخش ان در شبکه جلوگیری مینماید
۴. از امنیت فایلها و عدم دسترسی افراد غیر مجاز، اطمینان حاصل می گردد
۵. سیستم کامپیوتری در محیطی نصب می شود که نسبت به آب، گرد و غبار، رطوبت و تغییرات دما و تجاوزات فیزیکی آسیب ناپذیر باشد.
۶. سیستم هشدار دهنده مناسب برای آتش، آب و تغییرات هوا نصب گردیده
۷. اطلاعات پزشکی فقط توسط پرسنل مجاز در پرونده رایانه ای بیماران وارد میشود
۸. کاربرها قبل از دسترسی به اطلاعات سیستم، یک رمز اختصاصی را وارد می نمایند
۹. کاربران در هنگام ثبت اطلاعات بخصوص پرونده های بیماران، دقت نموده و از بروز اشتباه در ثبت جلوگیری می نمایند
۱۰. کاربران تمامی اطلاعات در نظر گرفته شده در برنامه را به صورت دقیق و کامل ثبت می نمایند
۱۱. دستیابی به محیط کامپیوتر منوط به اجازه نامه می باشد و در حد امکان تعداد افراد مجاز به حداقل رسیده
۱۲. تغییر عبارات رمز، زمانی که هر کارمند قسمت کامپیوتری از این واحد انتقال می یابد و همینطور تغییر عبارات رمز به صورت دوره ای انجام می پذیرد
۱۳. تمام پرسنل بخشهای دیگر جز قسمت کامپیوتر، در زمان حضور در مرکز کامپیوتر تحت نظر می باشند
۱۴. لیستی از تعداد و موقعیت کامپیوترهای موجود در بیمارستان و محتویات داخلی آنها تهیه شده است
۱۵. با توجه به اینکه کلیه سیستمهای این بیمارستان بصورت domain میباشند تمای سیاستهای امنیتی از بالا به پایین یعنی از Serve به Client اعمال میگردد
۱۶. از طریق سرور مرکزی هفته ای یکبار از کلیه اطلاعات back up تهیه می کند.
۱۷. از طریق لوح فشرده نسخه پشتیبان تهیه می کند
۱۸. درب ورودی اتاق سرور را قفل می نماید.
۱۹. کاربران هیچگومه دخل و تصرفی در این زمینه ندارند.
۲۰. با واگذاری نام کاربر و پسورد اختصاصی و همچنین سطح دسترسی هر واحد و هر کاربر به اطلاعات ، عملکرد کاربران مدیریت میشود.

کارشناسان مدیریت اطلاعات

۱. بدون اجازه صریح مدیر مدارک پزشکی نمی توان ازپرونده های پزشکی رونوشت برداشت
۲. فقط پرسنل بخش مدارک پزشکی مجاز به ذخیره و بازیابی پرونده هستند
۳. مدارک پزشکی در جایی نگهداری می شود که تنها برای پرسنل مجاز قابل دسترسی است
۴. پرسنل مدارک پزشکی از اصول محرمانه بودن مدارک پزشکی، مطابق قانون و از استانداردهای حرفه ای و خط مشی های تعیین شده توسط مسئولین بهداشتی و درمانی، در این زمینه حمایت و پیروی می کنند
۵. کاربران واحد مدارک پزشکی پس از هر بار استفاده از برنامه خارج شده و کاربری خود را غیر فعال می نمایند.
۶. تمام کاربران با رمز ورود خود وارد نرم افزار HIS بیمارستان می شوند
۷. کارشناس مدارک پزشکی از ورود افراد متفرقه به بخش مدارک پزشکی خودداری می کنند

مستندات مرتبط:

تهیه کننده:	تایید کننده:	تصویب کننده:
مسئول مدیریت اطلاعات سلامت	مدیریت بیمارستان	ریاست بیمارستان