دانشگاه علوم پزشکی و خدمات بهداشتی درمانی کرمانشاه

مدیریت آمارو فناوری اطلاعات

شیوه نامه عمومی نظارت و ارزیابی شرایط امنیتی حاکم بر شبکه داده ها و تجهیزات سخت افزاری و سامانه های نرم افزاری

۱. کسب اطمینان کامل از نصب و معتبر بودن و بروزرسانی آنتی ویروی پادویش بر روی کلیه سیستم ها و سرور ها.
۲. نصب و بروزرسانی بسته ی امنیتی بر روی سیستم عامل ها و تجهیزات شبکه ای سرویس دهنده .
۳. مدیریت حساب های کاربری اینترنت بر اساس دستور العمل موجود در ساب پرتال مدیریت فناوری اطلاعات و انتخاب رمز عبور با پیچیدگی مناسب برای آنها.
۴. عدم ارایه دسترسی از راه دور جهت امور نگهداری و پشتیبانی مگر در مواقع ضروری و بصورت کنترل شده(حذف دسترسی های ذخیره شده از راه دور و عدم ارایه دسترسی بدون امکان مشاهده کارشناسان دانشگاه (remote desktop).
۵. تهیه منظم پشتیبان از داده ها و تنظیمات و نگهداری بر روی رسانه های ذخیره سازی متعدد و جدا سازی فیزیکی از سرور میزبان و انجام مانور بازیابی پشتیبان
۶. بازبینی و مدیریت حساب های کاربری برروی کلیه سیستم عامل ها و حذف کلیه اکانت های متفرقهو تغییر رمز عبور در بازه های زمانی مشخص و مستند سازی و ارایه مستندات به مدیریت حراست.
۷. جداسازی شبکه کنترل تجهیزات پزشکی از شبکه متصل به اینترنت.
۸. تهیه یک نسخه از پشتیبان داده ها بر روی مدیا مطمئن و تحویل همراه با صورت جلسه به حراست واحد مربوطه.
۹. تهیه و پیش بینی یک دستگاه سرور برای مدیریت در شرایط بحران.
۱۰. انجام استعلام امنیتی از مدیریت حراست برای پیمانکاران قدیم و جدید و کارکنان مربوطه.
۱۱. غیر فعال کردن اینترنت سرور های HIS و سرور هایی که نیازمند outcoming service نیستند.
۱۲. فعال سازی فایروال نرم افزاری یا سخت افزاری بر سر راه دسترسی به سرویس های مستقر در مراکز.
۱۳. هماهنگی و مشورت با کارشناسان مدیریت فناوری اطلاعات در صورت مشاهده رفتارها، فایل ها و اکانت های مشکوک. بر روی سرور ها و تجهیزات.
۱۴. پایش فیزیکال اتاق سرور و توجه به مواردی از قبیل: آلارم های سخت افزاری بر روی تجهیزات – ارتینگ - برق ذخیره - برق پشتیبان - کنترل ورود و خروج به فضا اتاق سرور و سیستم اعلام و اطفا حریق.